



Your reliable networking solutions partner

User's Guide

Vigor2110 Series Broadband Firewall Router User's Guide

Version: 1.1 Date: 24/08/2009



Copyright Information

Copyright Declarations	Copyright 2009 All rights reserved. This publication contains information that is protected by copyright. No part may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language without written permission from the copyright holders.
Trademarks	 The following trademarks are used in this document: Microsoft is a registered trademark of Microsoft Corp. Windows, Windows 95, 98, Me, NT, 2000, XP, Vista and Explorer are trademarks of Microsoft Corp. Apple and Mac OS are registered trademarks of Apple Inc. Other products may be trademarks or registered trademarks of their respective manufacturers.

Safety Instructions and Approval

Safety	• Read the installation guide thoroughly before you set up the router.
Instructions	• The router is a complicated electronic unit that may be repaired only be authorized and qualified personnel. Do not try to open or repair the router yourself.
	 Do not place the router in a damp or humid place, e.g. a bathroom. The router should be used in a sheltered area, within a temperature range of +5 to +40 Celsius.
	 Do not expose the router to direct sunlight or other heat sources. The housing and electronic components may be damaged by direct sunlight or heat sources. Do not deploy the cable for LAN connection outdoor to prevent electronic shock hazards.
	 Keep the package out of reach of children. When you want to dispose of the router, please follow local regulations on conservation of the environment.
Warranty	We warrant to the original end user (purchaser) that the router will be free from any defects in workmanship or materials for a period of two (2) years from the date of purchase from the dealer. Please keep your purchase receipt in a safe place as it serves as proof of date of purchase. During the warranty period, and upon proof of purchase, should the product have indications of failure due to faulty workmanship and/or materials, we will, at our discretion, repair or replace the defective products or components, without charge for either parts or labor, to whatever extent we deem necessary tore-store the product to proper operating condition. Any replacement will consist of a new or re-manufactured functionally equivalent product of equal value, and will be offered solely at our discretion. This warranty will not apply if the product is modified, misused, tampered with, damaged by an act of God, or subjected to abnormal working conditions. The warranty does not cover the bundled or licensed software of other vendors. Defects which do not significantly affect the usability of the product will not be covered by the warranty. We reserve the right to revise the manual and online documentation and to make changes from time to time in the contents hereof without obligation to notify any person of such revision or changes.
Be a Registered Owner	Web registration is preferred. You can register your Vigor router via http://www.draytek.com.
Firmware & Tools Updates	Due to the continuous evolution of DrayTek technology, all routers will be regularly upgraded. Please consult the DrayTek web site for more information on newest firmware, tools and documents.
	http://www.draytek.com



European Community Declarations

Manufacturer: DrayTek Corp.

Address:No. 26, Fu Shing Road, HuKou Township, HsinChu Industrial Park, Hsin-Chu, Taiwan 303Product:Vigor2110 Series Router

DrayTek Corp. declares that Vigor2110 Series of routers are in compliance with the following essential requirements and other relevant provisions of R&TTE Directive 1999/5/EEC.

The product conforms to the requirements of Electro-Magnetic Compatibility (EMC) Directive 2004/108/EC by complying with the requirements set forth in EN55022/Class B and EN55024/Class B.

The product conforms to the requirements of Low Voltage (LVD) Directive 2006/95/EC by complying with the requirements set forth in EN60950-1.

Regulatory Information

Federal Communication Commission Interference Statement

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions:

(1) This device may not cause harmful interference, and

(2) This device may accept any interference received, including interference that may cause undesired operation.

Please visit http://www.draytek.com/user/AboutRegulatory.php



This product is designed for POTS and 2.4GHz WLAN network throughout the EC region and Switzerland with restrictions in France. Please see the user manual for the applicable networks on your product.

Table of Contents



Preface	1
1.1 Web Configuration Buttons Explanation	1
1.2 LED Indicators and Connectors	
1.2.1 For Vigor2110 1.2.2 For Vigor2110n 1.2.3 For Vigor2110Vn	2
1.3 Hardware Installation	8
Stand Installation	9
1.4 Printer Installation	10



Configuring Basic Settings	.15
2.1 Two-Level Management	15
2.2 Accessing Web Page	15
2.3 Changing Password	16
2.4 Quick Start Wizard	18
2.4.2 PPPoE 2.4.3 PPTP 2.4.4 Static IP 2.4.5 DHCP	20 21
2.5 Online Status	23
2.6 Saving Configuration	24



User Mode Operation	25
3.1 Internet Access	25
 3.1.1 Basics of Internet Protocol (IP) Network 3.1.2 PPPoE 3.1.3 Static or Dynamic IP 3.1.4 PPTP/L2TP 	27
3.2 LAN	35
3.2.1 Basics of LAN 3.2.2 General Setup	35 36
3.3 NAT	39
3.3.1 Port Redirection 3.3.2 DMZ Host 3.3.3 Open Ports	41
3.4 Applications	45
3.4.1 Dynamic DNS	45



3.4.2 UPnP	47
3.5 VoIP	49
3.5.1 DialPlan 3.5.2 SIP Accounts 3.5.3 Phone Settings	60
3.5.4 Status	
3.6 Wireless LAN	69
 3.6.1 Basic Concepts. 3.6.2 General Setup. 3.6.3 Security. 3.6.4 Access Control. 3.6.5 Station List 	
3.7 System Maintenance	
 3.7.1 System Status 3.7.2 User Password 3.7.3 Time and Date 3.7.4 Reboot System 	
3.8 Diagnostics	80
3.8.1 DHCP Table 3.8.2 Traffic Graph 3.8.3 Ping Diagnosis 3.8.4 Trace Route	81 81



Admin Mode Operation	83
4.1 Internet Access	83
 4.1.1 Basics of Internet Protocol (IP) Network 4.1.2 PPPoE 4.1.3 Static or Dynamic IP 4.1.4 PPTP/L2TP 	85 87
4.2 LAN	93
 4.2.1 Basics of LAN 4.2.2 General Setup 4.2.3 Static Route 4.2.4 VLAN 4.2.5 Bind IP to MAC 	95 98 101
4.3 NAT	103
4.3.1 Port Redirection 4.3.2 DMZ Host 4.3.3 Open Ports	106
4.4 Hardware Acceleration	110
4.5 Firewall	111
 4.5.1 Basics for Firewall 4.5.2 General Setup 4.5.3 Filter Setup 4.5.4 DoS Defense 	113 115
4.6 Objects Settings	123
4.6.1 IP Object	123



4.5.2 IP Group	125
4.6.3 Service Type Object	
4.5.4 Service Type Group	
4.6.5 Keyword Object	
4.5.6 Keyword Group	
4.6.7 File Extension Object 4.6.8 IM Object	
4.6.9 P2P Object	
4.6.10 Misc Object	
4.7 CSM Profile	
4.7.1 IM/P2P Filter Profile	137
4.7.2 URL Content Filter Profile	
4.7.3 Web Content Filter Profile	142
4.8 Bandwidth Management	144
4.8.1 Sessions Limit	
4.8.2 Bandwidth Limit	
4.8.3 Quality of Service	
•	
4.9 Applications	
4.9.1 Dynamic DNS	
4.9.2 Schedule	
4.9.3 RADIUS	
4.9.4 UPnP	
4.9.5 IGMP 4.9.6 Wake on LAN	
4.10 VPN and Remote Access	162
4.10.1 Remote Access Control	162
4.10.2 PPP General Setup	
4.10.3 IPSec General Setup	163
.10.4 IPSec Peer Identity	
4.10.5 Remote Dial-in User	
4.10.6 LAN to LAN	
4.10.7 Connection Management	
4.11 Certificate Management	178
4.11.1 Local Certificate	178
4.11.2 Trusted CA Certificate	
4.11.3 Certificate Backup	
4.12 VoIP	101
4.12.1 DialPlan	
4.12.2 SIP Accounts	
4.12.3 Phone Settings	
4.12.4 Status	
4.13 Wireless LAN	200
4.13.1 Basic Concepts	200
4.13.2 General Setup	
4.13.3 Security	206
4.13.4 Access Control	
4.13.5 WPS	
4.13.6 WDS	
4.13.7 Advanced Setting.	
4.13.8 WMM Configuration	
4.13.9 AP Discovery 4.13.10 Station List	



4.14 System Maintenance	217
4.12.1 System Status	
4.14.2 TR-069	219
4.14.3 Administrator Password	220
4.14.4 Configuration Backup	221
4.14.5 Syslog/Mail Alert	223
4.14.6 Time and Date	
4.14.7 Management	
4.14.8 Reboot System	226
4.14.9 Firmware Upgrade	
4.15 Diagnostics	
-	
4.15.1 Dial-out Trigger	
4.15.1 Dial-out Trigger 4.15.2 Routing Table 4.15.3 ARP Cache Table	
4.15.1 Dial-out Trigger 4.15.2 Routing Table 4.15.3 ARP Cache Table	
4.15.1 Dial-out Trigger 4.15.2 Routing Table 4.15.3 ARP Cache Table 4.15.4 DHCP Table	
 4.15.1 Dial-out Trigger 4.15.2 Routing Table 4.15.3 ARP Cache Table 4.15.4 DHCP Table 4.15.5 NAT Sessions Table 	
 4.15.1 Dial-out Trigger	228 229 229 230 230 230 231
 4.15.1 Dial-out Trigger 4.15.2 Routing Table 4.15.3 ARP Cache Table 4.15.4 DHCP Table 4.15.5 NAT Sessions Table 4.15.6 Data Flow Monitor 4.15.7 Traffic Graph 	228 229 229 230 230 231 231 232
 4.15.1 Dial-out Trigger	228 229 229 230 230 231 232 232 233



Application and Examples	.235
5.1 Create a LAN-to-LAN Connection Between Remote Office and Headquarter	. 235
5.2 Create a Remote Dial-in User Connection Between the Teleworker and Headquarter	. 242
5.3 QoS Setting Example	. 246
5.4 LAN – Created by Using NAT	. 249
5.5 Calling Scenario for VoIP function	. 252
5.5.1 Calling via SIP Sever 5.5.2 Peer-to-Peer Calling	252 254
5.6 Upgrade Firmware for Your Router	. 255
5.7 Request a certificate from a CA server on Windows CA Server	. 258
5.8 Request a CA Certificate and Set as Trusted on Windows CA Server	. 262



Trouble Shooting	265
6.1 Checking If the Hardware Status Is OK or Not	265
6.2 Checking If the Network Connection Settings on Your Computer Is OK or Not	266
6.3 Pinging the Router from Your Computer	268
6.4 Checking If the ISP Settings are OK or Not	269
6.5 Problems for 3G Network Connection	271
6.6 Backing to Factory Default Setting If Necessary	272
6.6 Contacting Your Dealer	273





Vigor2110 series is a broadband router. It integrates IP layer QoS, NAT session/bandwidth management to help users control works well with large bandwidth.

By adopting hardware-based VPN platform and hardware encryption of AES/DES/3DS, the router increases the performance of VPN greatly, and offers several protocols (such as IPSec/PPTP/L2TP) with up to 2 VPN tunnels.

The object-based design used in SPI (Stateful Packet Inspection) firewall allows users to set firewall policy with ease. CSM (Content Security Management) provides users control and management in IM (Instant Messenger) and P2P (Peer to Peer) more efficiency than before. By the way, DoS/DDoS prevention and URL/Web content filter strengthen the security outside and control inside.

Object-based firewall is flexible and allows your network be safe. In addition, through VoIP function, the communication fee for you and remote people can be reduced.

In addition, Vigor2110 series supports USB interface for connecting USB printer to share printer or USB storage device for sharing files. Vigor2110 series provides two-level management to simplify the configuration of network connection. The user mode allows user accessing into WEB interface via simple configuration. However, if users want to have advanced configurations, they can access into WEB interface through admin mode.

1.1 Web Configuration Buttons Explanation

Several main buttons appeared on the web pages are defined as the following:

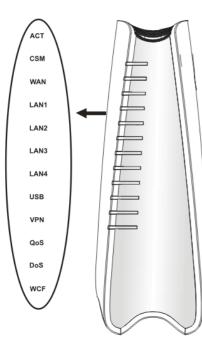
ОК	Save and apply current settings.
Cancel	Cancel current settings and recover to the previous saved settings.
Clear	Clear all the selections and parameters settings, including selection from drop-down list. All the values must be reset with factory default settings.
Add	Add new settings for specified item.
Edit	Edit the settings for the selected item.
Delete	Delete the selected item with the corresponding settings.
Note: For the or explanation.	ther buttons shown on the web pages, please refer to Chapter 4 for detailed



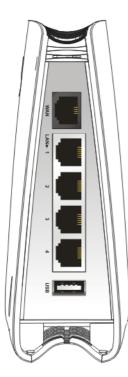
1.2 LED Indicators and Connectors

Before you use the Vigor router, please get acquainted with the LED indicators and connectors first.

1.2.1 For Vigor2110



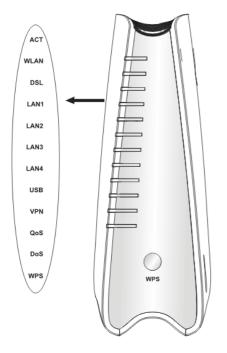
LED	Status	Explanation
ACT	Blinking	The router is powered on and running
(Activity)		normally.
VAN On Blin AN 1/2/3/4 JSB On JSB On Blin /PN On QoS On DoS On Blin VCF On	Off	The router is powered off.
CSM	On	The profile(s) of CSM (Content Security
		Management) for IM/P2P, URL/Web
		Content Filter application can be enabled
		from Firewall >>General Setup. (Such
		profile must be established under CSM
WAN	On	menu).
W AIN	-	The WAN port is connected.
	<u> </u>	It will blink while transmitting data.
I AN 1/2/3/4		The port is connected.
LAN 1/2/3/4		The port is disconnected.
LICD	Blinking	The data is transmitting.
CSM WAN LAN 1/2/3/4 USB VPN QoS DoS WCF Interface WAN LAN (1-4) USB	-	A USB device is connected and active.
	Blinking	The data is transmitting.
		The VPN tunnel is active.
QoS	On	The QoS function is active.
DoS	On	The DoS/DDoS function is active.
	Blinking	It will blink while detecting an attack.
WCF	On	The profile(s) of CSM (Content Security
		Management) for Web Content Filter
		application can be enabled from Firewall
		>>General Setup. (Such profile must be
Intorfago	Decorinti	established under CSM menu)
	Descripti	
		for accessing the Internet.
		s for local networked devices.
USB		for USB storage device (Pen Driver/Mobile
	HD) or pri	mer.



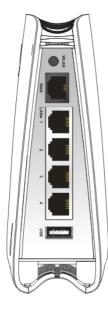


Interface	Description
Factory Reset	Restore the default settings. Usage: Turn on the router (ACT LED is blinking). Press the hole and keep for more than 5 seconds. When you see the ACT LED begins to blink rapidly than usual, release the button. Then the router will restart with the factory default configuration.
PWR	Connector for a power adapter.
ON/OFF	Power Switch.

1.2.2 For Vigor2110n



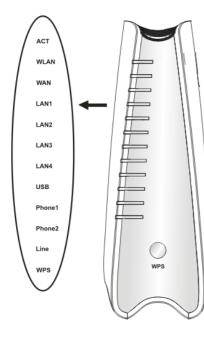
LED	Status	Explanation		
ACT	Blinking	The router is powered on and running		
(Activity)	Dillikilig	normally.		
(neuvity)	Off	The router is powered off.		
WLAN	On	Wireless access point is ready.		
	Blinking	It will blink while wireless traffic goes		
	Dilliking	through.		
WAN	On	The WAN port is connected.		
	Blinking	It will blink while transmitting data.		
	On	The port is connected.		
LAN 1/2/3/4	Off	The port is disconnected.		
	Blinking	The data is transmitting.		
USB	On	A USB device is connected and active.		
0.02	Blinking	The data is transmitting.		
VPN	On	The VPN tunnel is active.		
QoS	On	The QoS function is active.		
	-	The DoS/DDoS function is active.		
DoS	On Diation			
WDC	Blinking	It will blink while detecting an attack.		
WPS	On	The WPS is on.		
	Off	The WPS is off.		
	Blinking	Waiting for wireless client sending requests for connection about two minutes.		
WPS Button	0			
WPS Button	On	Press this button for 2 seconds to wait for client device making network connection		
		through WPS. When the LED lights up, the		
		WPS will be on.		
	Off	The WPS is off.		
	Blinking	Waiting for wireless client sending requests		
	0	for connection about two minutes.		
Interface	Descripti	on		
WLAN		utton once to enable (WLAN LED on) or		
	disable (W	LAN LED off) wireless connection.		
WAN	Connector	for accessing the Internet.		
LAN (1-4)	Connecters	Connecters for local networked devices.		
USB	Connecter	for USB storage (Pen Driver Mobile/HD) or		
	printer.			



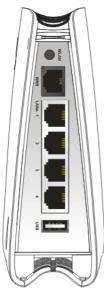


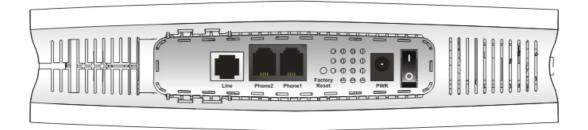
Interface	Description
Factory Reset	Restore the default settings. Usage: Turn on the router (ACT LED is blinking). Press the hole and keep for more than 5 seconds. When you see the ACT LED begins to blink rapidly than usual, release the button. Then the router will restart with the factory default configuration.
PWR	Connecter for a power adapter.
ON/OFF	Power Switch.

1.2.3 For Vigor2110Vn



LED	Status	Explanation
ACT		
ACT (Activity)	Blinking	The router is powered on and running normally.
(Activity)	Off	The router is powered off.
WLAN	On	Wireless access point is ready.
W LAIN		It will blink while wireless traffic goes
	Blinking	through.
WAN	On	The WAN port is connected.
W7111	Blinking	It will blink while transmitting data.
	On	The port is connected.
LAN 1/2/3/4	Off	The port is connected.
	Blinking	The data is transmitting.
USB	On	A USB device is connected and active.
USD	Blinking	The data is transmitting.
Phone1/	On	0
Phone2	Off	The phone connected to this port is off-hook.
T Home2		The phone connected to this port is on-hook.
Line	Blinking	A phone call comes.
Line	On	A PSTN phone call comes (in and out). However, when the phone call is
		disconnected, the LED will be off about six
		seconds later.
•	Off	There is no PSTN phone call.
WPS	On	The WPS is on.
	Off	The WPS is off.
•	Blinking	Waiting for wireless client sending requests
	0	for connection about two minutes.
WPS Button	On	Press this button for 2 seconds to wait for
		client device making network connection
		through WPS. When the LED lights up, the
·		WPS will be on.
	Off	The WPS is off.
	Blinking	Waiting for wireless client sending requests
		for connection about two minutes.
Interface	Description	
WLAN		utton once to enable (WLAN LED on) or LAN LED off) wireless connection.
XX / A X /		
WAN		for accessing the Internet.
LAN (1-4)		for local networked devices.
USB		for USB storage (Pen Driver Mobile/HD) or
	printer.	



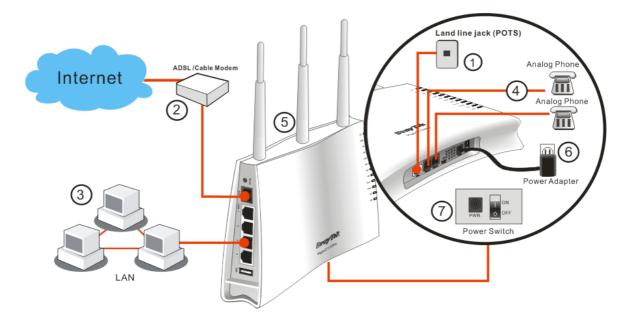


Interface	Description
Line	Connector for PSTN life line.
Phone2/Phone1	Connecter of analog phone for VoIP communication.
Factory Reset	Restore the default settings. Usage: Turn on the router (ACT LED is blinking). Press the hole and keep for more than 5 seconds. When you see the ACT LED begins to blink rapidly than usual, release the button. Then the router will restart with the factory default configuration.
PWR	Connecter for a power adapter.
ON/OFF	Power Switch.

1.3 Hardware Installation

Before starting to configure the router, you have to connect your devices correctly.

- 1. Connect Line port to land line jack with a RJ-11 cable (Vn model).
- 2. Connect this device to a modem with a RJ-45 cable.
- 3. Connect one port of 4-port switch to your computer with a RJ-45 cable. This device allows you to connect 4 PCs directly.
- 4. Connect Phone port to a conventional analog telephone.
- 5. Connect detachable antennas to the router for Vigor2110 series (n model).
- 6. Connect one end of the power cord to the power port of this device. Connect the other end to the wall outlet of electricity.
- 7. Power on the router.
- 8. Check the ACT and WAN, LAN LEDs to assure network connections.



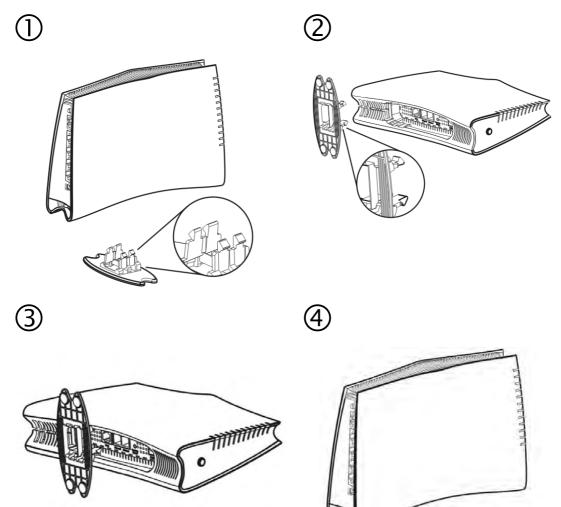
Caution:

 Each of the Phone ports can be connected to an analog phone only. Do not connect the phone ports to the land line jack. Such connection might damage your router.
 When the power is shutdown, VoIP phone will be disconnected. However, a phone set connected to Phone 2 port can be used as the traditional telephone for the line will be guided to land line jack via the router (loop through).



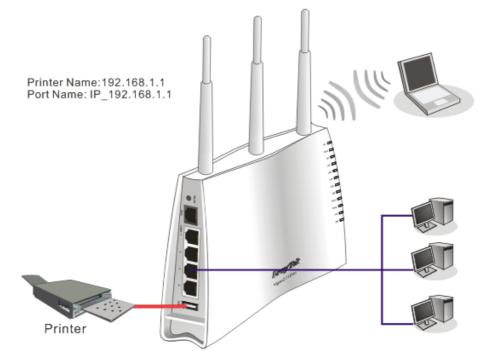
Stand Installation

The Vigor2110 must be placed erectly. Therefore you have to install a stand onto the router to make it standing firmly. Please follow the figures listed below to finish the installation.



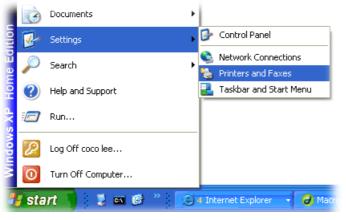
1.4 Printer Installation

You can install a printer onto the router for sharing printing. All the PCs connected this router can print documents via the router. The example provided here is made based on Windows XP/2000. For Windows 98/SE/Vista, please visit **www.draytek.com**.



Before using it, please follow the steps below to configure settings for connected computers (or wireless clients).

- 1. Connect the printer with the router through USB/parallel port.
- 2. Open Start->Settings-> Printer and Faxes.



3. Open File->Add Printer. A welcome dialog will appear. Please click Next.



4. Click Local printer attached to this computer and click Next.

d Printer Wizard Local or Network Printer	1
The wizard needs to know wh	hich type of printer to set up.
Select the option that describe	es the printer you want to use:
Ocal printer attached to th	his computer
Automatically detect a	nd install my Plug and Play printer
To set up a network use the "Local printe	printer that is not attached to a print server, #"option.
	< Back Next > Cancel

5. In this dialog, choose **Create a new port Type of port** and use the drop down list to select **Standard TCP/IP Port**. Click **Next**.

elect a Printer Port Computers communicate v	with printers through ports.	6
Select the port you want yo new port.	our printer to use. If the port is not listed, you	can create a
OUse the following port:	LPT1: (Recommended Printer Port)	1
The connector for this	port should look something like this:	
000		
© <u>C</u> reate a new port: Type of port:	Standard TCP/IP Port	

6. In the following dialog, type **192.168.1.1** (router's LAN IP) in the field of **Printer Name** or **IP Address** and type **IP_192.168.1.1** as the port name. Then, click **Next**.

dd Port For which device do you wan	t to add a port?
Enter the Printer Name or IP a	ddress, and a port name for the desired device.
Printer Name or IP Address:	192.168.1.1
Port Name:	IP_192.168.1.1

7. Click Standard and choose Generic Network Card.

dd Standard TC	CP/IP Printer Port Wizard 🛛 🔀
	t Information Required
1. The device is p	vice is of unknown type. Be sure that properly configured. In the previous page is correct.
	address and perform another search on the network by returning to the age or select the device type if you are sure the address is correct.
Device Type	
(Standard	Generic Network Card
Ocustom	Settings
	< <u>B</u> ack <u>N</u> ext > Cancel

8. Then, in the following dialog, click **Finish**.



9. Now, your system will ask you to choose right name of the printer that you installed onto the router. Such step can make correct driver loaded onto your PC. When you finish the selection, click **Next**.

I he manufacturer an	d model determine which printer software to use.	Ø
	cturer and model of your printer. If your printer came isk. If your printer is not listed, consult your printer d	
compatible printer	software.	
Manufacturer	Printers	
AST AT&T	Brother HL-1060 BR-Script2 Brother HL-1070 BR-Script2	4
Brother	Brother HL-1070	
Bull Canon	Bromer HL-TUPS7DPS	
This driver is digitally si		Have Disk
Tell me why driver sign	ing is important	

10. For the final stage, you need to go back to **Control Panel-> Printers** and edit the property of the new printer you have added.

Br	other HL-1070		
Print to the fo checked por		nts will print to the first free	
Port	Description	Printer	3
□ 3.250 □ IP_1	Standard TCP/IP Port Standard TCP/IP Port	Epson Stylus COLOR 1160	1
0 IP_1	Standard TCP/IP Port Standard TCP/IP Port Standard TCP/IP Port	HP LaserJet 1300	
☑ IP_1	Standard TCP/IP Port Standard TCP/IP Port Local Port	Brother HL-1070 PDF995	
Add P	ort Delete	e Port Configure Port	
Enable bio	directional support		_

11. Select "LPR" on Protocol, type **p1** (number 1) as Queue Name. Then click **OK**. Next please refer to the red rectangle for choosing the correct protocol and UPR name.

ort Settings		
Port Name:	IP_192.168.1.1	
Printer Name or IP <u>A</u> ddress:	192.168.1.1	
Protocol O <u>B</u> aw	(OLP	0
Raw Settings		
Port Number	91.00	
LPR Settings	-	-
Queue Name:	abled	
SNMP Status Enabled	1	
Community Name.	public	1
SNMP Device Index:	1	

The printer can be used for printing now. Most of the printers with different manufacturers are compatible with vigor router.

Note 1: Some printers with the fax/scanning or other additional functions are not supported. If you do not know whether your printer is supported or not, please visit www.draytek.com to find out the printer list. Open **Support >FAQ**; find out the link of **Printer Server** and click it; then click the **What types of printers are compatible with Vigor router?** link.

AQ - Basic		FAQ
AQ - Dasic		FAQ
01. What are the differences among thes	e firmware file formats ?	Basic
02. How could I get the telnet command	for routers ?	Advanced
)3. How can I backup/restore my configu	VPN	
) J4. How do I reset/clear the router's pas	sword ?	DHCP
D5. How to bring back my router to its de	efault value ?	Wireless
D6. How do I tell the type of my Vigor Ro	uter is AnnexA or AnnexB? (For ADSL model only)	VoIP
)7. Ways for firmware upgrade.		QoS
	3.6 and above for Vigor2200 Series routers?	ISDN
		Firewall / IP Filter
)9. I failed to upgrade Vigor Router's firm	ware from my Mac machine constantly, what should	Printer Server

FAQ - Printer Server

01. How do I configure LPR printing on Windows2000/XP ?

02. How do I configure LPR printing on Windows98/Me ?

03. How do I configure LPR printing on Linux boxes ?

04. Why there are some strange print-out when I try to print my documents through Vigor210 4P / 2300's print server?

05. What types of printers are compatible with Vigor router?

06. What are the limitations in the USB Printer Port of Vigor Router ?

07. What is the printing buffer size of Vigor Router ?

08. How do I configure LPR printing on Mac OSX ?

09. How do I configure LPR printing on My Windows Vista ?

Note 2: Vigor router supports printing request from computers via LAN ports but not WAN port.



2 Configuring Basic Settings

For using the router properly, it is necessary for you to change the password of web configuration for security and adjust primary basic settings.

2.1 Two-Level Management

This chapter explains how to setup a password for an administrator/user and how to adjust basic/advanced settings for accessing Internet successfully.

For user mode operation, do not type any word on the window and click **Login** for the simple web pages for configuration. Yet, for admin mode operation, please type "admin/admin" on Username/Password and click **Login** for full configuration.

2.2 Accessing Web Page

- 1. Make sure your PC connects to the router correctly.
 - 8

Notice: You may either simply set up your computer to get IP dynamically from the router or set up the IP address of the computer to be the same subnet as **the default IP address of Vigor router 192.168.1.1**. For the detailed information, please refer to the later section - Trouble Shooting of the guide.

2. Open a web browser on your PC and type **http://192.168.1.1.** The following window will be open to ask for username and password.

Username Password	
Copyright©, DrayTek Corp. All	Login Rights Reserved. DrayTek

3. For user mode operation, do not type any word on the window and click **Login** for the simple web pages for configuration. Yet, for admin mode operation, please type "admin/admin" on Username/Password and click **Login** for full configuration.



Notice: If you fail to access to the web configuration, please go to "Trouble Shooting" for detecting and solving your problem.

4. The web page can be logged out according to the chosen condition. The default setting is **Auto Logout**, which means the web configuration system will logout after 5 minutes without any operation. Change the setting for your necessity.



Γ	Auto Logout 🔽
Γ	Auto Loqout
ŀ	Off 👘
Ŀ	1 min
k	3 min 🗧
ļ	5 min
ŀ	10 min

2.3 Changing Password

No matter user mode operation or admin mode operation, please change the password for the original security of the router.

- 1. Open a web browser on your PC and type **http://192.168.1.1.** A pop-up window will open to ask for username and password.
- 2. Please type "admin/admin" on Username/Password for admin mode. Otherwise, do not type any word (both username and password are Null for user mode) on the window and click **Login** on the window.
- 3. Now, the **Main Screen** will appear.

Auto Logout 💙	System Status			
nline Status	Model Name Firmware Version Build Date/Time	: Vigor2110 series : 3.3.1 : Jul 29 2009 17:05:31		
AN AT ardware Acceleration irewall bjects Setting SM	MAC Address 1st IP Address 1st Subnet Mask DHCP Server DNS	LAN : 00-50-7F-9A-32-70 : 192.168.1.1 : 255.255.255.0 : Yes : 168.95.1.1	Link Status MAC Address Connection IP Address Default Gateway	WAN 1 : Connected : 00-50-7F-9A-32-71 : DHCP Client : 192.168.5.29 : 192.168.5.1
andwidth Management pplications PN and Remote Access ertificate Management olP /ireless LAN ystem Maintenance iagnostics	Port Profil Phone1 Phone2	VoIP e Reg. In/Out No 0/0 No 0/0	MAC Address Frequency Domain Firmware Version SSID	eless LAN : 00-50-7F-9A-32-70 : Europe : 1.8.1.0 : DrayTek

Main screen for admin mode operation (full configuration)

Land Wadel Name : Vigor2110 series Firmware Version : 3.3.1 Build Date/Time : Jul 29 2009 17:05:31 N T T MAC Address Dications : 00-50-7F-9A-32-70 1st IP Address : 192.168.1.1 DHC Server : Yes DHS : 168.95.1.1 DNS : 192.168.5.29 Default Gateway : 192.168.5.1	to Logout 💌		System Status			
MAC Address : 00-50-7F-9A-32-70 Link Status : Connected Mac Address : 192.168.1.1 MAC Address : 00-50-7F-9A-32-70 Ist IP Address : 192.168.1.1 MAC Address : 00-50-7F-9A-32-71 Ist Subnet Mask : 255.255.25.0 IP Address : 192.168.5.29 DHCP Server : Yes IP Address : 192.168.5.1 gnostics VOIP Wireless LAN Port Profile Reg. In/Out Phone1 No 0/0 Frequency Domain : Europe Phone2 No 0/0 Frequency Domain : Europe	ine Status rnet Access	_	Firmware Version	: 3.3.1		
MAC Address : 00-50-7F-9A-32-70 Link Status : Connected P 1st IP Address : 192.168.1.1 MAC Address : 00-50-7F-9A-32-70 Ist IP Address : 192.168.1.1 MAC Address : 00-50-7F-9A-32-71 Ist Subnet Mask : 255.255.255.0 Connection : DHCP Client DHCP Server : Yes IP Address : 192.168.5.29 DNS : 168.95.1.1 Default Gateway : 192.168.5.1 Port Portipe Wireless LAN Phone1 No 0/0 Frequency Domain Phone2 No 0/0 Firmware Version : 1.8.1.0				LAN		WAN 1
VoIP Wireless LAN Port Profile Reg. In/Out Phone1 No 0/0 Frequency Domain : Europe Phone2 No 0/0 Firmware Version : 1.8.1.0	lications o eless LAN tem Maintenance		1st IP Address 1st Subnet Mask DHCP Server	: 192.168.1.1 : 255.255.255.0 : Yes	MAC Address Connection IP Address	: 00-50-7F-9A-32-71 : DHCP Client : 192.168.5.29
Phone1 No 0/0 Frequency Domain : Europe Phone2 No 0/0 Firmware Version : 1.8,1.0	gnostics	=		VoIP	Wir	eless LAN
			Phone1	No 0/0	Frequency Domain Firmware Version	: 1.8.1.0

Main screen for user mode operation (simple configuration)

Note: The home page will change slightly in accordance with the type of the router you have.

4. Go to **System Maintenance** page and choose **Administrator Password/User Password**.

OI	d Password				
Ne	ew Password				
Co	onfirm Password				
		0	V I		
		or			
System Maintenar	nce >> User Passwo	or			
	nce >> User Passwo	or	<u> </u>		
User Password	nce >> User Passwor Id Password	or			
<mark>User Password</mark> O		or			

- 5. Enter the login password (the default is blank) on the field of **Old Password**. Type **New Password**. Then click **OK** to continue.
- 6. Now, the password has been changed. Next time, use the new password to access the Web Configurator for this router.



System Maintenance >> Administrator Password Setup

Username Password	Login
Copyright©, DrayTek Corp. All	Rights Reserved. Dray Tek

2.4 Quick Start Wizard

0

Notice: Quick Start Wizard for user mode operation is the same as for admin mode operation.

If your router can be under an environment with high speed NAT, the configuration provide here can help you to deploy and use the router quickly. The first screen of **Quick Start Wizard** is entering login password. After typing the password, please click **Next**.

Quick Start Wizard

Enter login password	
Please enter an alpha-numeric strin	ng as your Password (Max 23 characters).
Old Password	
New Password	
Confirm Password	
1	
	<pre></pre>

On the next page as shown below, please select the appropriate Internet access type according to the information from your ISP. For example, you should select PPPoE mode if the ISP provides you PPPoE interface. Then click **Next** for next step.

Quick Start Wizard

Connect to Inter	net

WAN 1				
Select one of the following Internet Acces	ss types provid	ed by your ISP	ч.	
PPPoE				
○ РРТР				
🔘 Static IP				
O DHCP				
	< Back	Next >	Finish	Cance

2.4.2 PPPoE

PPPoE stands for **Point-to-Point Protocol over Ethernet**. It relies on two widely accepted standards: PPP and Ethernet. It connects users through an Ethernet to the Internet with a common broadband medium, such as a single DSL line, wireless device or cable modem. All the users over the Ethernet can share a common connection.

PPPoE is used for most of DSL modem users. All local users can share one PPPoE connection for accessing the Internet. Your service provider will provide you information about user name, password, and authentication mode.

If your ISP provides you the **PPPoE** connection, please select **PPPoE** for this router. The following page will be shown:

Quick Start Wizard

PPPoE Client Mode WAN 1						
	er name and pas	sword provided by	your ISP.			
User Name		123	123			
Password		•••				
Confirm Pas	sword	•••				
		<	< Back	Next >	Finish	Cancel
User Name	Assign	a specific valid	user nam	e provided	l by the ISF	.
Password	Assign	a valid passwor	d provide	d by the Is	SP.	

Confirm Password Retype the password.

Click Next for viewing summary of such connection.

Quick Start Wizard

WAN Interface:	WAN1
Physical Mode:	Ethernet
Physical Type:	Auto negotiation
Internet Access:	PPPoE
Click Back to modify cha settings and restart the V	nges if necessary. Otherwise, click Finish to save the current 'igor router.

Click Finish. Then, the system status of this protocol will be shown.

2.4.3 PPTP

Click **PPTP** as the protocol. Type in all the information that your ISP provides for this protocol.

Quick Start Wizard

WAN 1		
Enter the user name, pass your ISP.	vord, WAN IP configuration and PPTP server IP provided b	ру
User Name	123	
Password	•••	
Confirm Password	•••	
WAN IP Configuration		
💿 Obtain an IP address	automatically	
🔘 Specify an IP address		
IP Address		
Subnet Mask		
Gateway	undefined	
Primary DNS	undefined	
Second DNS	undefined	
PPTP Server		

Click Next for viewing summary of such connection.



Qu	ick	Start	W	izaro	d
-					

WAN Interface:	1414814
	WAN1
Physical Mode:	Ethernet
Physical Type:	Auto negotiation
Internet Access:	РРТР
Click Back to modify chan settings and restart the V	nges if necessary. Otherwise, click Finish to save the current rigor router.

Click **Finish.** Then, the system status of this protocol will be shown.

2.4.4 Static IP

Click **Static IP** as the protocol. Type in all the information that your ISP provides for this protocol.

Quick Start Wizard

WAN 1		
Enter the Static IP config	uration probided by your ISP	
WAN IP	172.16.3.229	
Subnet Mask	255.255.0.0	
Gateway	172.16.3.4	
Primary DNS		
Secondary DNS		(optional)

After finishing the settings in this page, click **Next** to see the following page.

e confirm your settings:	
WAN Interface:	WAN1
Physical Mode:	Ethernet
Physical Type:	Auto negotiation
Internet Access:	Static IP
settings and restart the V	
	<pre>< Back Next > Finish Ca</pre>

Click **Finish.** Then, the system status of this protocol will be shown.

2.4.5 DHCP

Click **DHCP** as the protocol. Type in all the information that your ISP provides for this protocol.

Quick Start Wizard

DHCP Client Mode	
WAN 1	uires you to enter a specific host name or specific MAC address, please
enter it in.	anes you to enter a specific flost flame of specific MAC address, please
Host Name	(optional)
MAC	00 -50 -7F -92 -F5 -61 (optional)
1	
	<pre>< Back Next > Finish Cancel</pre>

After finishing the settings in this page, click **Next** to see the following page.

Quick Start Wizard

Please confirm your settings:	
WAN Interface:	WAN1
Physical Mode:	Ethernet
Physical Type:	Auto negotiation
Internet Access:	DHCP
Click Back to modify char settings and restart the Vi	nges if necessary. Otherwise, click Finish to save the current igor router.
	< Back Next > Finish Cancel

Click Finish. Then, the system status of this protocol will be shown.

2.5 Online Status

The online status shows the system status, WAN status, and other status related to this router within one page. If you select **PPPoE/PPPoA** as the protocol, you will find out a link of **Dial PPPoE** or **Drop PPPoE** in the Online Status web page.

Online status for DHCP

Online Status

System Status				Syster	m Uptime: 4:7:24
LAN Status	Primary	y DNS: 172.16	.3.18	Secondary DN	S: 168.95.1.1
IP Address	TX Packets	RX Pac	kets		
192.168.1.5	21848	32232			
WAN Status					>> <u>Release</u>
Enable	Line	Name	Mode	Up Time	
Yes	Ethernet		DHCP Client	4:07:16	
IP	GW IP	TX Packets	TX Rate(Bps)	RX Packets	RX Rate(Bps)
192.168.5.26	192.168.5.1	10538	11	10547	26

Detailed explanation is shown below:

Primary DNS	Displays the IP address of the primary DNS.
Secondary DNS	Displays the IP address of the secondary DNS.
LAN Status	
IP Address	Displays the IP address of the LAN interface.
TX Packets	Displays the total transmitted packets at the LAN interface.
RX Packets	Displays the total number of received packets at the LAN interface.
WAN Status	
Line	Displays the physical connection (Ethernet) of this interface.

Name	Displays the name set in WAN1/WAN web page.	
Mode	Displays the type of WAN connection (e.g., PPPoE).	
Up Time	Displays the total uptime of the interface.	
IP	Displays the IP address of the WAN interface.	
GW IP	Displays the IP address of the default gateway.	
TX Packets	Displays the total transmitted packets at the WAN interface.	
TX Rate	Displays the speed of transmitted octets at the WAN interface.	
RX Packets	Displays the total number of received packets at the WAN interface.	
RX Rate	Displays the speed of received octets at the WAN interface.	
RX Rate	Displays the speed of received octets at the WAN interface.	

Note: The words in green mean that the WAN connection of that interface is ready for accessing Internet; the words in red mean that the WAN connection of that interface is not ready for accessing Internet.

2.6 Saving Configuration

Each time you click **OK** on the web page for saving the configuration, you can find messages showing the system interaction with you.

Status: Ready

Ready indicates the system is ready for you to input settings.

Settings Saved means your settings are saved once you click Finish or OK button.

3 User Mode Operation

This chapter will guide users to execute simple configuration through user mode operation. As for other examples of application, please refer to chapter 5.

- 1. Open a web browser on your PC and type **http://192.168.1.1.** The window will ask for typing username and password.
- 2. **Do not** type any word (both username and password are Null for user operation) on the window and click **Login** on the window.

Now, the **Main Screen** will appear. Be aware that "User mode" will be displayed on the bottom left side.

Ist IP Address . 192/106.1.1 Connection : DHCP Client Ist Subnet Mask : 255.255.255.0 DHCP Server : Yes DNS : 168.95.1.1 Default Gateway : 192.168.5.1 Stics VoIP Profile Reg. In/Out MAC Address : 00-50-7F-9A-3
MAC Address : 00-50-7F-9A-32-70 Link Status : Connected Ist IP Address : 192.168.1.1 MAC Address : 00-50-7F-9A-32 Ist Subnet Mask : 255.255.255.0 Connection : DHCP Client DHCP Server : Yes Default Gateway : 192.168.5.1 Stics VOIP Wireless LAN Port Profile Reg. In/Out
ittions 1st IP Address : 192.168.1.1 MAC Address : 00-50-7F-9A-32 ist LAN DHCP Server : 255.255.0 Connection : DHCP Client DHCP Server : Yes DHCP Client IP Address : 192.168.5.29 bits DHS : 168.95.1.1 Default Gateway : 192.168.5.1 VoIP Wireless LAN Wireless LAN Port Profile Reg. In/Out
VoIP Wireless LAN Port Profile Reg. In/Out MAC Address : 00-50-7F-9A-3
Phone1 No 0/0 Frequency Domain : Europe Phone2 No 0/0 Firmware Version : 1.8.1.0 SSID : DrayTek

3.1 Internet Access

Quick Start Wizard offers user an easy method to quick setup the connection mode for the router. Moreover, if you want to adjust more settings for different WAN modes, please go to **Internet Access** group.

3.1.1 Basics of Internet Protocol (IP) Network

IP means Internet Protocol. Every device in an IP-based Network including routers, print server, and host PCs, needs an IP address to identify its location on the network. To avoid address conflicts, IP addresses are publicly registered with the Network Information Centre (NIC). Having a unique IP address is mandatory for those devices participated in the public network but not in the private TCP/IP local area networks (LANs), such as host PCs under the management of a router since they do not need to be accessed by the public. Hence, the NIC has reserved certain addresses that will never be registered publicly. These are known as *private* IP addresses, and are listed in the following ranges:



From 10.0.0.0 to 10.255.255.255 From 172.16.0.0 to 172.31.255.255 From 192.168.0.0 to 192.168.255.255

What are Public IP Address and Private IP Address

As the router plays a role to manage and further protect its LAN, it interconnects groups of host PCs. Each of them has a private IP address assigned by the built-in DHCP server of the Vigor router. The router itself will also use the default **private IP** address: 192.168.1.1 to communicate with the local hosts. Meanwhile, Vigor router will communicate with other network devices through a **public IP** address. When the data flow passing through, the Network Address Translation (NAT) function of the router will dedicate to translate public/private addresses, and the packets will be delivered to the correct host PC in the local area network. Thus, all the host PCs can share a common Internet connection.

Get Your Public IP Address from ISP

In ADSL deployment, the PPP (Point to Point)-style authentication and authorization is required for bridging customer premises equipment (CPE). Point to Point Protocol over Ethernet (PPPoE) connects a network of hosts via an access device to a remote access concentrator or aggregation concentrator. This implementation provides users with significant ease of use. Meanwhile it provides access control, billing, and type of service according to user requirement.

When a router begins to connect to your ISP, a serial of discovery process will occur to ask for a connection. Then a session will be created. Your user ID and password is authenticated via **PAP** or **CHAP** with **RADIUS** authentication system. And your IP address, DNS server, and other related information will usually be assigned by your ISP.

Network Connection by 3G USB Modem

For 3G mobile communication through Access Point is popular more and more, Vigor2110 adds the function of 3G network connection for such purpose. By connecting 3G USB Modem to the USB port of Vigor2110, it can support HSDPA/UMTS/EDGE/GPRS/GSM and the future 3G standard (HSUPA, etc). Vigor2110n with 3G USB Modem allows you to receive 3G signals at any place such as your car or certain location holding outdoor activity and share the bandwidth for using by more people. Users can use four LAN ports on the router to access Internet. Also, they can access Internet via 802.11n wireless function of Vigor2110n, and enjoy the powerful firewall, bandwidth management, VPN, VoIP features of Vigor2110n series.



After connecting into the router, 3G USB Modem will be regarded as the second WAN port. However, the original Ethernet WAN1 still can be used and Load-Balance can be done in the router. Besides, 3G USB Modem also can be used as backup device. Therefore, when WAN1 is not available, the router will use 3.5G for supporting automatically. The supported 3G USB



Modem will be listed on Draytek web site. Please visit www.draytek.com for more detailed information.

Below shows the menu items for Internet Access.



3.1.2 PPPoE

To choose PPPoE as the accessing protocol of the internet, please select **PPPoE** from the **Internet Access** menu. The following web page will be shown.

Internet Access >> PPPoE

PPPoE Client Mode			
PPPoE Setup		PPP/MP Setup	
PPPoE Link	🔘 Enable 💿 Disable	PPP Authentication	PAP or CHAP
ISP Access Setup		✓ Always On	
ISP Name		Idle Timeout	-1 second(s)
Username		IP Address Assignment Method	
Password		(IPCP) WAN IP Alias	5
		Fixed IP	🔘 Yes 💿 No (Dynamic IP)
WAN Connection Dete	ection	Fixed IP Address	
Mode	ARP Detect 🐱		
Ping IP		Oefault MAC Add	
TTL:		 Specify a MAC Address MAC Address: 00 .50 .7F .9A .32 .71 	
3G USB Modem			
Dial Backup Mode Disable 💙			
Go to <u>3G USB Modem</u> Setup			

Enable/Disable	Click Enable for activating this function. If you click Disable , this function will be closed and all the settings that you adjusted in this page will be invalid.
ISP Access Setup	Enter your allocated username, password and authentication parameters according to the information provided by your ISP. Username – Type in the username provided by ISP in this field. Password – Type in the password provided by ISP in this field. Index (1-15) in Schedule Setup - You can type in four sets of time schedule for your request. All the schedules can be set previously in Application – Schedule web page and you can use the number that you have set in that web page.
WAN Connection Detection	Such function allows you to verify whether network connection is alive or not through ARP Detect or Ping Detect. Mode – Choose ARP Detect or Ping Detect for the system to execute for WAN detection. Ping IP – If you choose Ping Detect as detection mode, you have to type IP address in this field for pinging.

OK



TTL (**Time to Live**) – Displays value for your reference. TTL value is set by telnet command.

WAN Backup Setup	3G USB Modem – If you install a 3G USB modem on the router		
	please Enable the Dial Backup Mode to perform file backup via		
	USB device. After choosing Enable, please click the 3G USB		
	Modem link to access into the following page for configuring		
	detailed settings.		

WAN >> Internet Access

3G USB Modem Setup		
PPP Client Mode	🔘 Enable 💿 Disable	
SIM PIN code		
Modem Initial String	AT&FE0V1X1&D2&C1S0=0	(Default:AT&FE0V1X1&D2&C1S0=0)
APN Name		Apply
Modem Dial String	ATDT*99#	(Default:ATDT*99#)
PPP Username		(Optional)
PPP Password		(Optional)
	OK Cancel	Default

PPP Client Mode - Click Enable to activate this mode for WAN2.

SIM PIN code - Type PIN code of the SIM card that will be used to access Internet.

Modem Initial String - Such value is used to initialize USB modem. Please use the default value. If you have any question, please contact to your ISP.

APN Name - APN(Access Point Name) is provided by your ISP for identifying different access points. Simply click **Apply** to apply such name. Finally, you have to click **OK** to save the setting. **Apply** – Activate the function of identification.

Modem Dial String - Such value is used to dial through USB mode. Please use the default value. If you have any question, please contact to your ISP.

PPP Username - Type the PPP username (optional).

PPP Password - Type the PPP password (optional).

PPP/MP SetupPPP Authentication – Select **PAP only** or **PAP or CHAP** for PPP.
If you want to connect to Internet all the time, you can check
Always On.
Idle Timeout – Set the timeout for breaking down the Internet after
passing through the time without any action.**IP Address**Usually ISP dynamically assigns IP address to you each time you

Assignment Method
(IPCP)Ostanly isr dynamically assigns in address to you each time you
connect to it and request. In some case, your ISP provides service to
always assign you the same IP address whenever you request. In this
case, you can fill in this IP address in the Fixed IP field. Please
contact your ISP before you want to use this function.

WAN IP Alias - If you have multiple public IP addresses and would like to utilize them on the WAN interface, please use WAN IP Alias. You can set up to 8 public IP addresses other than the current one you are using. Notice that this setting is available for WAN1 only.

ą	http://19	92.168.1.5	- WAN IP Alias - Microsoft Inte	rnet Explorer 🛛 🔲 🔀
	WAN IF	Alias (Multi-NAT)	
	Index	Enable	Aux, WAN IP	Join NAT IP Pool
	1.	v	172.16.3.229	v
	2.			
	з.			
	4.			
	5.			
	6.			
	7.			
	8.			
	1		OK Clear All	Close

Fixed IP – Click **Yes** to use this function and type in a fixed IP address in the box of **Fixed IP Address**.

Default MAC Address – You can use **Default MAC Address** or specify another MAC address by typing on the boxes of MAC Address for the router.

Specify a MAC Address – Type the MAC address for the router manually.

After finishing all the settings here, please click **OK** to activate them.

3.1.3 Static or Dynamic IP

For static IP mode, you usually receive a fixed public IP address or a public subnet, namely multiple public IP addresses from your DSL or Cable ISP service providers. In most cases, a Cable service provider will offer a fixed public IP, while a DSL service provider will offer a public subnet. If you have a public subnet, you could assign an IP address or many IP address to the WAN interface.

To use **Static or Dynamic IP** as the accessing protocol of the internet, please choose **Static or Dynamic IP** mode from **Internet Access** menu. The following web page will be shown.



Internet Access >> Static or Dynamic IP

Static or Dynamic IP (DHCP Client)

Access Control	WAN IP Network Settings WAN IP Alias
Broadband Access 💿 Enable 🔿 Disable	Obtain an IP address automatically
Keep WAN Connection Enable PING to keep alive	Router Name * Domain Name *
PING to the IP 0.0.0.0	* : Required for some ISPs O Specify an IP address
PING Interval 0 minute(s)	IP Address 192.168.5.29
WAN physical type	Subnet Mask 255.255.255.0
Auto negotiation 💌	Gateway IP Address 192.168.5.1
WAN Connection Detection Mode ARP Detect Ping IP	 Default MAC Address Specify a MAC Address MAC Address: 00 .50 .7F :9A .32 .71
RIP Protocol	DNS Server IP Address
Enable RIP	Primary IP Address Secondary IP Address
WAN Backup Setup 3G USB Modem Dial Backup Mode Disable ♥ Go to <u>3G USB Modem</u> Setup	

OK

Access Control	Click Enable for activating this function. If you click Disable , this function will be closed and all the settings that you adjusted in this page will be invalid.
Keep WAN Connection	Normally, this function is designed for Dynamic IP environments because some ISPs will drop connections if there is no traffic within certain periods of time. Check Enable PING to keep alive box to activate this function. PING to the IP - If you enable the PING function, please specify the IP address for the system to PING it for keeping alive. PING Interval - Enter the interval for the system to execute the PING operation.
WAN Physical Type	Choose Auto negotiation as the physical type for your router.
WAN Connection Detection	 Such function allows you to verify whether network connection is alive or not through ARP Detect or Ping Detect. Mode – Choose ARP Detect or Ping Detect for the system to execute for WAN detection. Ping IP – If you choose Ping Detect as detection mode, you have to type IP address in this field for pinging. TTL (Time to Live) – Displays value for your reference. TTL value is set by telnet command.

RIP Protocol	Routing Information Protocol is abbreviated as RIP (RFC1058) specifying how routers exchange routing tables information. Click Enable RIP for activating this function.
WAN Backup Setup	3G USB Modem – If you install a 3G USB modem on the router, please Enable the Dial Backup Mode to perform file backup via USB device. After choosing Enable, please click the 3G USB Modem link to access into the following page for configuring detailed settings.

WAN >> Internet Access

PPP Client Mode	🔘 Enable 💿 Disable	
SIM PIN code		
Modem Initial String	AT&FE0V1X1&D2&C1S0=0	(Default:AT&FE0V1X1&D2&C1S0=0)
APN Name		Apply
Modem Dial String	ATDT*99#	(Default:ATDT*99#)
PPP Username		(Optional)
PPP Password		(Optional)

PPP Client Mode - Click Enable to activate this mode for WAN2.

SIM PIN code - Type PIN code of the SIM card that will be used to access Internet.

Modem Initial String - Such value is used to initialize USB modem. Please use the default value. If you have any question, please contact to your ISP.

APN Name - APN(Access Point Name) is provided by your ISP for identifying different access points. Simply click **Apply** to apply such name. Finally, you have to click **OK** to save the setting. **Apply** – Activate the function of identification.

Modem Dial String - Such value is used to dial through USB mode. Please use the default value. If you have any question, please contact to your ISP.

PPP Username - Type the PPP username (optional).

PPP Password - Type the PPP password (optional).

This group allows you to obtain an IP address automatically and allows you type in IP address manually.

WAN IP Alias - If you have multiple public IP addresses and would like to utilize them on the WAN interface, please use WAN IP Alias. You can set up to 8 public IP addresses other than the current one you are using.

WAN IP Network

Settings



ø	http://19	92.168.1.5	- WAN IP Alias - Microsoft Inter	net Explorer 🛛 🔲 🔀
			naulat araw N	
		Enable	Multi-NAT) Aux. WAN IP	Join NAT IP Pool
			172.16.3.229	
	1.	v	172.10.3.229	V
	2.			
	з.			
	4.			
	5.			
	6.			
	7.			
	8.			
			OK Clear All	Close

Obtain an IP address automatically – Click this button to obtain the IP address automatically if you want to use **Dynamic IP** mode. *Router Name:* Type in the router name provided by ISP. *Domain Name:* Type in the domain name that you have assigned.

Specify an IP address – Click this radio button to specify some data if you want to use **Static IP** mode.

IP Address: Type the IP address.

Subnet Mask: Type the subnet mask.

Gateway IP Address: Type the gateway IP address.

Default MAC Address : Click this radio button to use default MAC address for the router.

Specify a MAC Address: Some Cable service providers specify a specific MAC address for access authentication. In such cases you need to click the **Specify a MAC Address** and enter the MAC address in the MAC Address field.

DNS Server IP
AddressType in the primary IP address for the router if you want to use
Static IP mode. If necessary, type in secondary IP address for
necessity in the future.

3.1.4 PPTP/L2TP

To use **PPTP/L2TP** as the accessing protocol of the internet, please choose **PPTP/L2TP** from **Internet Access** menu. The following web page will be shown.

Int	terne	et Ac	cess	>>	PPT	Р

PPTP Client Mode		
PPTP Setup	PPP Setup	
PPTP Link 🛛 🔿 Enable 💿 Disable	PPP Authentication	PAP or CHAP
PPTP Server	Always On	
ISP Access Setup	Idle Timeout	-1 second(s)
Username	IP Address Assign	nment Method (IPCP)
	Fixed IP	🔘 Yes 💿 No (Dynamic IP)
Password	Fixed IP Address	
	WAN IP Network S	Settings
WAN Backup Setup	Obtain an IP ad	Idress automatically
3G USB Modem	Specify an IP a	ddress
Dial Backup Mode Disable 🚩	IP Address	192.168.5.29
Go to <u>3G USB Modem Backup</u> Setup	Subnet Mask	255.255.255.0

OK

PPTP Setup	 Enable - Click this radio button to enable a PPTP client to establish a tunnel to a DSL modem on the WAN interface. Disable - Click this radio button to close the connection through PPTP. PPTP Server - Specify the IP address of the PPTP/L2TP server if you enable PPTP/L2TP client mode.
ISP Access Setup	Username -Type in the username provided by ISP in this field. Password -Type in the password provided by ISP in this field.
WAN Backup Setup	3G USB Modem – If you install a 3G USB modem on the router, please Enable the Dial Backup Mode to perform file backup via USB device. After choosing Enable, please click the 3G USB Modem Backup link to access into the following page for configuring detailed settings.

WAN >> Internet Access

PPP Client Mode	🔘 Enable 💿 Disable	
SIM PIN code		
Modem Initial String	AT&FE0V1X1&D2&C1S0=0	(Default:AT&FE0V1X1&D2&C1S0=0)
APN Name		Apply
Modem Dial String	ATDT*99#	(Default:ATDT*99#)
PPP Username		(Optional)
PPP Password		(Optional)

	PPP Client Mode - Click Enable to activate this mode for WAN2.
	SIM PIN code - Type PIN code of the SIM card that will be used to access Internet.
	Modem Initial String - Such value is used to initialize USB modem. Please use the default value. If you have any question, please contact to your ISP.
	 APN Name - APN(Access Point Name) is provided by your ISP for identifying different access points. Simply click Apply to apply such name. Finally, you have to click OK to save the setting. Apply – Activate the function of identification.
	Modem Dial String - Such value is used to dial through USB mode. Please use the default value. If you have any question, please contact to your ISP.
	PPP Username - Type the PPP username (optional).
	PPP Password - Type the PPP password (optional)
PPP Setup	PPP Authentication - Select PAP only or PAP or CHAP for PPP.
-	Idle Timeout - Set the timeout for breaking down the Internet after passing through the time without any action.
IP Address Assignment Method(IPCP)	Idle Timeout - Set the timeout for breaking down the Internet after
Assignment	 Idle Timeout - Set the timeout for breaking down the Internet after passing through the time without any action. Fixed IP - Usually ISP dynamically assigns IP address to you each time you connect to it and request. In some case, your ISP provides service to always assign you the same IP address whenever you request. In this case, you can fill in this IP address in the Fixed IP field. Please contact your ISP before you want to use this function. Click Yes to use this function and type in a fixed IP address in the
Assignment	 Idle Timeout - Set the timeout for breaking down the Internet after passing through the time without any action. Fixed IP - Usually ISP dynamically assigns IP address to you each time you connect to it and request. In some case, your ISP provides service to always assign you the same IP address whenever you request. In this case, you can fill in this IP address in the Fixed IP field. Please contact your ISP before you want to use this function. Click Yes to use this function and type in a fixed IP address in the box.

Dray Tek

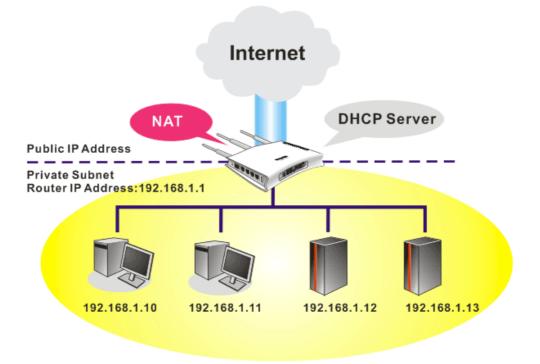
3.2 LAN

Local Area Network (LAN) is a group of subnets regulated and ruled by router. The design of network structure is related to what type of public IP addresses coming from your ISP.



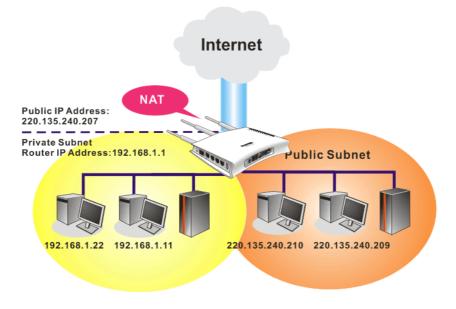
3.2.1 Basics of LAN

The most generic function of Vigor router is NAT. It creates a private subnet of your own. As mentioned previously, the router will talk to other public hosts on the Internet by using public IP address and talking to local hosts by using its private IP address. What NAT does is to translate the packets from public IP address to private IP address to forward the right packets to the right host and vice versa. Besides, Vigor router has a built-in DHCP server that assigns private IP address to each local host. See the following diagram for a briefly understanding.



In some special case, you may have a public IP subnet from your ISP such as 220.135.240.0/24. This means that you can set up a public subnet or call second subnet that each host is equipped with a public IP address. As a part of the public subnet, the Vigor router will serve for IP routing to help hosts in the public subnet to communicate with other public hosts or servers outside. Therefore, the router should be set as the gateway for public hosts.





What is Routing Information Protocol (RIP)

Vigor router will exchange routing information with neighboring routers using the RIP to accomplish IP routing. This allows users to change the information of the router such as IP address and the routers will automatically inform for each other.

3.2.2 General Setup

LAN >> General Setup

This page provides you the general settings for LAN.

Click LAN to open the LAN settings page and choose General Setup.

LAN IP Network Confi	guration	DHCP Server	Configurat	tion	
For NAT Usage		💿 Enable Serv	er 🔘 Disab	le Server	
1st IP Address 192.168.1.5		Relay Agent: (Relay Agent: 🔘 1st Subnet 🕕 2nd Subnet		
1st Subnet Mask	255.255.255.0	Start IP Addres	55	192.168.1.10	
For IP Routing Usage (🔵 Enable 💿 Disable	IP Pool Counts		50	
2nd IP Address	192.168.2.1	Gateway IP Ad	dress	192.168.1.5	
2nd Subnet Mask	255.255.255.0	DHCP Server IF	Address		
	2nd Subnet DHCP Server	for Relay Ager	nt		
		DNS Server IF	Address		
RIP Protocol Control	Disable 🔽	🔲 Force DNS	manual set	ting	
		Primary IP Add	ress		
		Secondary IP /	∖ddress		

1st IP Address	Type in private IP address for connecting to a local private network (Default: 192.168.1.1).
1st Subnet Mask	Type in an address code that determines the size of the network. (Default: 255.255.255.0/ 24)
For IP Routing Usage	Click Enable to invoke this function. The default setting is Disable .



2 nd IP Address	Type in secondary IP address for connecting to a subnet. (Default: 192.168.2.1/24)
2 nd Subnet Mask	An address code that determines the size of the network. (Default: 255.255.255.0/ 24)
2 nd DHCP Server	You can configure the router to serve as a DHCP server for the 2nd

subnet.

Start IP Ad	rver ddress	
IP Pool Co		10)
Index	Matched MAC Address	given IP Address
MAC Addre	ess : : : : : : : : : : : : : : : : : :	it Cancel

Start IP Address: Enter a value of the IP address pool for the DHCP server to start with when issuing IP addresses. If the 2nd IP address of your router is 220.135.240.1, the starting IP address must be 220.135.240.2 or greater, but smaller than 220.135.240.254.

IP Pool Counts: Enter the number of IP addresses in the pool. The maximum is 10. For example, if you type 3 and the 2nd IP address of your router is 220.135.240.1, the range of IP address by the DHCP server will be from 220.135.240.2 to 220.135.240.11.

MAC Address: Enter the MAC Address of the host one by one and click **Add** to create a list of hosts to be assigned, deleted or edited IP address from above pool. Set a list of MAC Address for 2nd DHCP server will help router to assign the correct IP address of the correct subnet to the correct host. So those hosts in 2nd subnet won't get an IP address belonging to 1st subnet.

RIP Protocol Control

Disable deactivates the RIP protocol. It will lead to a stoppage of the exchange of routing information between routers. (Default)

RIP Protocol Control



1st Subnet - Select the router to change the RIP information of the 1st subnet with neighboring routers.

2nd Subnet - Select the router to change the RIP information of the 2nd subnet with neighboring routers.



DHCP Server Configuration	DHCP stands for Dynamic Host Configuration Protocol. The router by factory default acts a DHCP server for your network so it automatically dispatch related IP settings to any local user configured as a DHCP client. It is highly recommended that you leave the router enabled as a DHCP server if you do not have a DHCP server for your network.
	If you want to use another DHCP server in the network other than the Vigor Router's, you can let Relay Agent help you to redirect the DHCP request to the specified location. Enable Server - Let the router assign IP address to every host in the LAN.
	Disable Server – Let you manually assign IP address to every host in the LAN.
	 Relay Agent – (1st subnet/2nd subnet) Specify which subnet that DHCP server is located the relay agent should redirect the DHCP request to. Start IP Address - Enter a value of the IP address pool for the DHCP server to start with when issuing IP addresses. If the 1st IP address of your router is 192.168.1.1, the starting IP address must be 192.168.1.2 or greater, but smaller than 192.168.1.254.
	 IP Pool Counts - Enter the maximum number of PCs that you want the DHCP server to assign IP addresses to. The default is 50 and the maximum is 253. Gateway IP Address - Enter a value of the gateway IP address for the DHCP server. The value is usually as same as the 1st IP address of the router, which means the router is the default gateway. DHCP Server IP Address for Relay Agent - Set the IP address of the DHCP server you are going to use so the Relay Agent can help to forward the DHCP request to the DHCP server.
DNS Server Configuration	DNS stands for Domain Name System. Every Internet host must have a unique IP address, also they may have a human-friendly, easy to remember name such as www.yahoo.com. The DNS server converts the user-friendly name into its equivalent IP address.
	 Force DNS manual setting - Force Vigor router to use DNS servers in this page instead of DNS servers given by the Internet Access server (PPPoE, PPTP, L2TP or DHCP server). Primary IP Address - You must specify a DNS server IP address here because your ISP should provide you with usually more than one DNS Server. If your ISP does not provide it, the router will automatically apply default DNS Server IP address: 194.109.6.66 to this field. Secondary IP Address - You can specify secondary DNS server IP address here because your ISP often provides you more than one DNS Server. If your ISP does not provide it, the router will automatically apply default secondary DNS server IP address here because your ISP often provides you more than one DNS Server. If your ISP does not provide it, the router will automatically apply default secondary DNS Server IP address: 194.98.0.1 to this field. The default DNS Server IP address can be found via Online Status:
	System Status System Uptime: 5:11:9 LAN Status Primary DNS: 194.109.6.66 Secondary DNS: 168.95.1.1 IP Address TX Packets RX Packets 192.168.1.5 9326 9487

If both the Primary IP and Secondary IP Address fields are left empty, the router will assign its own IP address to local users as a DNS proxy server and maintain a DNS cache.

If the IP address of a domain name is already in the DNS cache, the router will resolve the domain name immediately. Otherwise, the router forwards the DNS query packet to the external DNS server by establishing a WAN (e.g. DSL/Cable) connection.

There are two common scenarios of LAN settings that stated in Chapter 5. For the configuration examples, please refer to that chapter to get more information for your necessity.

3.3 NAT

Usually, the router serves as an NAT (Network Address Translation) router. NAT is a mechanism that one or more private IP addresses can be mapped into a single public one. Public IP address is usually assigned by your ISP, for which you may get charged. Private IP addresses are recognized only among internal hosts.

When the outgoing packets destined to some public server on the Internet reach the NAT router, the router will change its source address into the public IP address of the router, select the available public port, and then forward it. At the same time, the router shall list an entry in a table to memorize this address/port-mapping relationship. When the public server response, the incoming traffic, of course, is destined to the router's public IP address and the router will do the inversion based on its table. Therefore, the internal host can communicate with external host smoothly.

The benefit of the NAT includes:

- Save cost on applying public IP address and apply efficient usage of IP address. NAT allows the internal IP addresses of local hosts to be translated into one public IP address, thus you can have only one IP address on behalf of the entire internal hosts.
- Enhance security of the internal network by obscuring the IP address. There are many attacks aiming victims based on the IP address. Since the attacker cannot be aware of any private IP addresses, the NAT function can protect the internal network.

On NAT page, you will see the private IP address defined in RFC-1918. Usually we use the 192.168.1.0/24 subnet for the router. As stated before, the NAT facility can map one or more IP addresses and/or service ports into different specified services. In other words, the NAT function can be achieved by using port mapping methods.

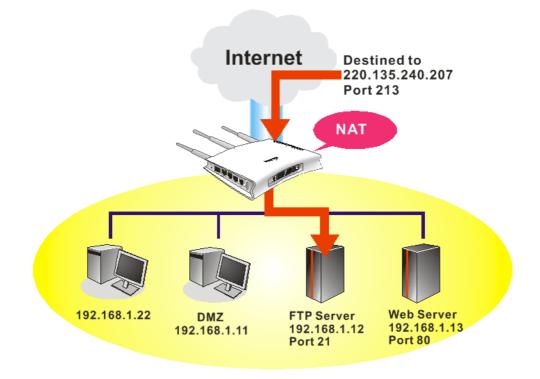
Below shows the menu items for NAT.



3.3.1 Port Redirection

Port Redirection is usually set up for server related service inside the local network (LAN), such as web servers, FTP servers, E-mail servers etc. Most of the case, you need a public IP address for each server and this public IP address/domain name are recognized by all users. Since the server is actually located inside the LAN, the network well protected by NAT of the router, and identified by its private IP address/port, the goal of Port Redirection function is to forward all access request with public IP address from external users to the mapping private IP address/port of the server.





The port redirection can only apply to incoming traffic.

To use this function, please go to **NAT** page and choose **Port Redirection** web page. The **Port Redirection Table** provides 20 port-mapping entries for the internal hosts.

Index	Service Name	Public Port	Private IP	Status
<u>1.</u>				х
<u>2.</u>				х
<u>3.</u>				х
<u>4.</u>				х
<u>5.</u>				х
<u>6.</u>				×
<u>7.</u>				х
<u>8.</u>				×
<u>9.</u>				х
<u>10.</u>				Х

NAT >> Port Redirection

Press any number under Index to access into next page for configuring port redirection.

Dray Tek

NAT >> Port Redirection

Index No. 1	
🗖 Enable	
Mode	Single 💌
Service Name	Single Range
Protocol	💙
WAN IP	1.All
Public Port	0
Private IP	
Private Port	0

Note: In "Range" Mode the End IP will be calculated automatically once the Public Port and Start IP have been entered.

	OK Clear Cancel
Enable	Check this box to enable such port redirection setting.
Mode	Two options (Single and Range) are provided here for you to choose. To set a range for the specific service, select Range . In Range mode, if the public port (start port and end port) and the starting IP of private IP had been entered, the system will calculate and display the ending IP of private IP automatically.
Service Name	Enter the description of the specific network service.
Protocol	Select the transport layer protocol (TCP or UDP).
WAN IP	Select the WAN IP used for port redirection. There are eight WAN IP alias that can be selected and used for port redirection. The default setting is All which means all the incoming data from any port will be redirected to specified range of IP address and port.
Public Port	Specify which port can be redirected to the specified Private IP and Port of the internal host. If you choose Range as the port redirection mode, you will see two boxes on this field. Simply type the required number on the first box. The second one will be assigned automatically later.
Private IP	Specify the private IP address of the internal host providing the service. If you choose Range as the port redirection mode, you will see two boxes on this field. Type a complete IP address in the first box (as the starting point) and the fourth digits in the second box (as the end point).
Private Port	Specify the private port number of the service offered by the internal host.

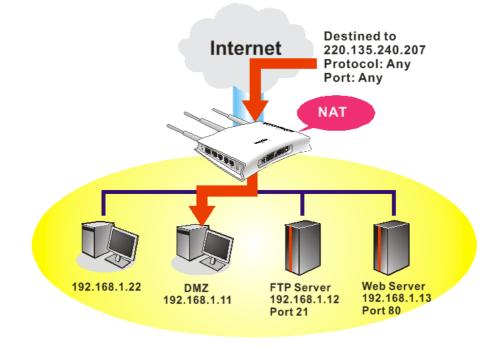
Note that the router has its own built-in services (servers) such as Telnet, HTTP and FTP etc. Since the common port numbers of these services (servers) are all the same, you may need to reset the router in order to avoid confliction.

3.3.2 DMZ Host

As mentioned above, **Port Redirection** can redirect incoming TCP/UDP or other traffic on particular ports to the specific private IP address/port of host in the LAN. However, other IP protocols, for example Protocols 50 (ESP) and 51 (AH), do not travel on a fixed port. Vigor router provides a facility **DMZ Host** that maps ALL unsolicited data on any protocol to a



single host in the LAN. Regular web surfing and other such Internet activities from other clients will continue to work without inappropriate interruption. **DMZ Host** allows a defined internal user to be totally exposed to the Internet, which usually helps some special applications such as Netmeeting or Internet Games etc.



The security properties of NAT are somewhat bypassed if you set up DMZ host. We suggest you to add additional filter rules or a secondary firewall.

Click **DMZ Host** to open the following page:

NIAT		DMZ	Linet	Cature
INA I	~~		nosi	Setup

VAN 1		
N	lone 💌	
Pr	rivate IP	Choose PC
м	AC Address of the True IP DMZ Host	
	ote: When a True-IP DMZ host is turned on a always on.	, it will force the router's WAN connection to

If you previously have set up **WAN Alias** for **PPPoE** or **Static or Dynamic IP** mode, you will find them in **Aux. WAN IP** for your selection.

NAT >> DMZ Host Setup

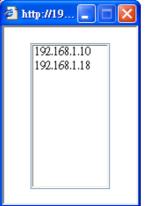
WAN 1 Index	Enable	Aux. WAN IP	Private IP	
1.		172.16.3.229		Choose PC
2.		162.168.1.55		Choose PC



Enable Check to enable the DMZ Host function.

Private IP Enter the private IP address of the DMZ host, or click Choose PC to select one.

Choose PC Click this button and then a window will automatically pop up, as depicted below. The window consists of a list of private IP addresses of all hosts in your LAN network. Select one private IP address in the list to be the DMZ host.



When you have selected one private IP from the above dialog, the IP address will be shown on the following screen. Click **OK** to save the setting.

NAT >> DMZ Host Setup

WAN 1				
Index	Enable	Aux, WAN IP	Private IP	
1.	V	172.16.3.229	192.168.1.10	Choose PC
2.		162.168.1.55		Choose PC

OK Clear

3.3.3 Open Ports

Open Ports allows you to open a range of ports for the traffic of special applications.

Common application of Open Ports includes P2P application (e.g., BT, KaZaA, Gnutella, WinMX, eMule and others), Internet Camera etc. Ensure that you keep the application involved up-to-date to avoid falling victim to any security exploits.

Click **Open Ports** to open the following page:

NAT >> Open Ports

Index	Comment	Aux, WAN IP	Local IP Address	Status
<u>1.</u>				×
<u>2.</u>				×
<u>3.</u>				×
<u>4.</u>				×
<u>5.</u>				×
<u>6.</u>				×
<u>7.</u>				×
<u>8.</u>				×
<u>9.</u>				×
<u>10.</u>				х

Index	Indicate the relative number for the particular entry that you want to offer service in a local host. You should click the appropriate index number to edit or clear the corresponding entry.
Comment	Specify the name for the defined network service.
Local IP Address	Display the private IP address of the local host offering the service.
Status	Display the state for the corresponding entry. X or V is to represent the Inactive or Active state.

To add or edit port settings, click one index number on the page. The index entry setup page will pop up. In each index entry, you can specify **10** port ranges for diverse services.

NAT >> Open Ports >> Edit Open Ports

✓ E	nable Ope	en Ports						
		Comme	ent	P2P				
		WAN I	P	172.	16.3.229	~		
		Local (Computer	192.	168.1.10	Choo	ise PC	
	Protoc	col	Start Port	End Port		Protocol	Start Port	End Port
1.	TCP	*	4500	4700	6.	💙	0	0
2.	UDP	*	4500	4700	7.	🔽	0	0
з.		*	0	0	8.	💙	0	0
4.		*	0	0	9.	💙	0	0
5.		~	0	0	10.	💙	0	0

Enable Open Ports	Check to enable this entry.
Comment	Make a name for the defined network application/service.
WAN IP	Specify the WAN IP address that will be used for this entry. This setting is available when WAN IP Alias is configured.
Local Computer	Enter the private IP address of the local host or click Choose PC to select one.
Choose PC	Click this button and, subsequently, a window having a list of private IP addresses of local hosts will automatically pop up. Select the appropriate IP address of the local host in the list.
Protocol	Specify the transport layer protocol. It could be TCP , UDP , or (none) for selection.
Start Port	Specify the starting port number of the service offered by the local host.
End Port	Specify the ending port number of the service offered by the local host.

3.4 Applications

Below shows the menu items for Applications.

Applications Dynamic DNS UPnP

3.4.1 Dynamic DNS

The ISP often provides you with a dynamic IP address when you connect to the Internet via your ISP. It means that the public IP address assigned to your router changes each time you access the Internet. The Dynamic DNS feature lets you assign a domain name to a dynamic WAN IP address. It allows the router to update its online WAN IP address mappings on the specified Dynamic DNS server. Once the router is online, you will be able to use the



registered domain name to access the router or internal virtual servers from the Internet. It is particularly helpful if you host a web server, FTP server, or other server behind the router.

Before you use the Dynamic DNS feature, you have to apply for free DDNS service to the DDNS service providers. The router provides up to three accounts from three different DDNS service providers. Basically, Vigor routers are compatible with the DDNS services supplied by most popular DDNS service providers such as **www.dyndns.org**, **www.no-ip.com**, **www.dtdns.com**, **www.changeip.com**, **www.dynamic- nameserver.com**. You should visit their websites to register your own domain name for the router.

Enable the Function and Add a Dynamic DNS Account

- 1. Assume you have a registered domain name from the DDNS provider, say *hostname.dyndns.org*, and an account with username: *test* and password: *test*.
- 2. In the DDNS setup menu, check **Enable Dynamic DNS Setup**.

Dynamic DNS Setup		1	Set to Factory Default
Enable Dynamic DNS	Setup	View Log	Force Update
Auto-Update interval	1440 Min(s)		
Accounts:			
Index	Domain Name		Active
<u>1.</u>			х
<u>2.</u>			x
<u>3.</u>			x

Applications >> Dynamic DNS Setup

OK	Clear All

Set to Factory Default	Clear all profiles and recover to factory settings.	
Enable Dynamic DNS Setu	Check this box to enable DDNS function.	
Auto-Update interval	Set the time for the router to perform auto update for DDNS service.	
Index	Click the number below Index to access into the setting page of DDNS setup to set account(s).	
Domain Name	Display the domain name that you set on the setting page of DDNS setup.	
Active	Display if this account is active or inactive.	
View Log	Display DDNS log status.	
Force Update	Force the router updates its information to DDNS server.	

3. Select Index number 1 to add an account for the router. Check **Enable Dynamic DNS Account**, and choose correct Service Provider: dyndns.org, type the registered hostname: *hostname* and domain name suffix: dyndns.org in the **Domain Name** block. The following two blocks should be typed your account Login Name: *test* and Password: *test*.



Index : 1 Enable Dynamic DNS	Account	
Service Provider	dyndns.org (www.dyndns.org)	*
Service Type	Dynamic 💌	
Domain Name	chronic6853 dyndns.org	dyndns.org 🖌
Login Name	chronic6853	(max. 64 characters)
Password	•••••	(max. 23 characters)
🔲 Wildcards		
📃 Backup MX		
Mail Extender		
	OK Clear	Cancel

Applications >> Dynamic DNS Setup >> Dynamic DNS Account Setup

Enable Dynamic DNS Account	Check this box to enable the current account. If you did check the box, you will see a check mark appeared on the Active column of the previous web page in step 2).
Service Provider	Select the service provider for the DDNS account.
Service Type	Select a service type (Dynamic, Custom or Static). If you choose Custom, you can modify the domain that is chosen in the Domain Name field.
Domain Name	Type in one domain name that you applied previously. Use the drop down list to choose the desired domain.
Login Name	Type in the login name that you set for applying domain.
Password	Type in the password that you set for applying domain.

4. Click **OK** button to activate the settings. You will see your setting has been saved.

The Wildcard and Backup MX features are not supported for all Dynamic DNS providers. You could get more detailed information from their websites.

Disable the Function and Clear all Dynamic DNS Accounts

In the DDNS setup menu, uncheck **Enable Dynamic DNS Setup**, and push **Clear All** button to disable the function and clear all accounts from the router.

Delete a Dynamic DNS Account

In the DDNS setup menu, click the **Index** number you want to delete and then push **Clear All** button to delete the account.

3.4.2 UPnP

The **UPnP** (Universal Plug and Play) protocol is supported to bring to network connected devices the ease of installation and configuration which is already available for directly connected PC peripherals with the existing Windows 'Plug and Play' system. For NAT routers, the major feature of UPnP on the router is "NAT Traversal". This enables applications inside the firewall to automatically open the ports that they need to pass through a router. It is more reliable than requiring a router to work out by itself which ports need to be opened. Further, the user does not have to manually set up port mappings or a DMZ. **UPnP is available on Windows XP** and the router provide the associated support for MSN Messenger to allow full use of the voice, video and messaging features.



Applications >> UPnP

UPnP
🗹 Enable UPnP Service
Enable Connection control Service
Enable Connection Status Service

Note: If you intend running UPnP service inside your LAN, you should check the appropriate service above to allow control, as well as the appropriate UPnP settings.

OK	Clear	Cancel
	oicui	Cancer

Enable UPNP Service

Accordingly, you can enable either the **Connection Control Service** or **Connection Status Service**.

After setting **Enable UPNP Service** setting, an icon of **IP Broadband Connection on Router** on Windows XP/Network Connections will appear. The connection status and control status will be able to be activated. The NAT Traversal of UPnP enables the multimedia features of your applications to operate. This has to manually set up port mappings or use other similar methods. The screenshots below show examples of this facility.

dress 🔕 Network Connections		😨 IP Broadband Connection or	n Router Status 📿 🖡
Network Tasks	Broadband	General	
Create a new connection Set up a home or small office network	hinet Disconnected WAN Miniport (PPPOE)	Internet Gateway Status:	Connected
	Dial-up	Duration:	00:19:06
See Also 🏦	test	Speed:	100.0 Mbps
Vetwork Troubleshooter Other Places	Internet Gateway	Activity Internet Internet Gatew	vay My Computer
Control Panel My. Network Places My Documents My Computer	IP Broadband Connection on Router Enabled	Packets: Sent: 404 Received: 1,115	734 666
Details (*) Network Connections System Folder	LAN or High-Speed Internet	Properties Disable	

The UPnP facility on the router enables UPnP aware applications such as MSN Messenger to discover what are behind a NAT router. The application will also learn the external IP address and configure port mappings on the router. Subsequently, such a facility forwards packets from the external ports of the router to the internal ports used by the application.

Dray Tek

ieneral	Services
Connect to the Internet using:	Select the services running on your network that Internet users can access.
Section on Router	Services
This connection allows you to connect to the Internet through a shared connection on another computer.	 ☐ Ftp Example ✓ msnmsgr (192.168.29.11:13135) 60654 UDP ✓ msnmsgr (192.168.29.11:7824) 13251 UDP ✓ msnmsgr (192.168.29.11:8789) 63231 TCP

The reminder as regards concern about Firewall and UPnP

Can't work with Firewall Software

Enabling firewall applications on your PC may cause the UPnP function not working properly. This is because these applications will block the accessing ability of some network ports.

Security Considerations

Activating the UPnP function on your network may incur some security threats. You should consider carefully these risks before activating the UPnP function.

- Some Microsoft operating systems have found out the UPnP weaknesses and hence you need to ensure that you have applied the latest service packs and patches.
- Non-privileged users can control some router functions, including removing and adding port mappings.

The UPnP function dynamically adds port mappings on behalf of some UPnP-aware applications. When the applications terminate abnormally, these mappings may not be removed.

3.5 VoIP

Voice over IP network (VoIP) enables you to use your broadband Internet connection to make toll quality voice calls over the Internet.

There are many different call signaling protocols, methods by which VoIP devices can talk to each other. The most popular protocols are SIP, MGCP, Megaco and H.323. These protocols are not all compatible with each other (except via a soft-switch server).

The Vigor V models support the SIP protocol as this is an ideal and convenient deployment for the ITSP (Internet Telephony Service Provider) and softphone and is widely supported. SIP is an end-to-end, signaling protocol that establishes user presence and mobility in VoIP structure. Every one who wants to talk using his/her SIP Uniform Resource Identifier, "SIP Address". The standard format of SIP URI is

sip: user:password @ host: port

Some fields may be optional in different use. In general, "host" refers to a domain. The "userinfo" includes the user field, the password field and the @ sign following them. This is very similar to a URL so some may call it "SIP URL". SIP supports peer-to-peer direct calling and also calling via a SIP proxy server (a role similar to the gatekeeper in H.323 networks),



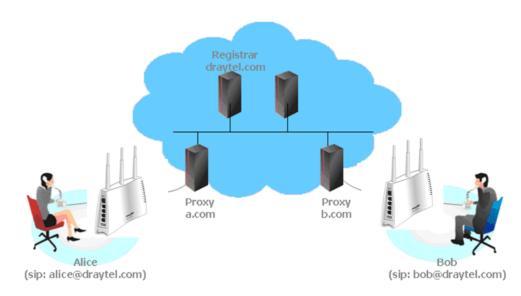
while the MGCP protocol uses client-server architecture, the calling scenario being very similar to the current PSTN/ISDN network.

After a call is setup, the voice streams transmit via RTP (Real-Time Transport Protocol). Different codecs (methods to compress and encode the voice) can be embedded into RTP packets. Vigor V models provide various codecs, including G.711 A/ μ -law, G.723, G.726 and G.729 A & B. Each codec uses a different bandwidth and hence provides different levels of voice quality. The more bandwidth a codec uses the better the voice quality, however the codec used must be appropriate for your Internet bandwidth.

Usually there will be two types of calling scenario, as illustrated below:

• Calling via SIP Servers

First, the Vigor V models of yours will have to register to a SIP Registrar by sending registration messages to validate. Then, both parties' SIP proxies will forward the sequence of messages to caller to establish the session.

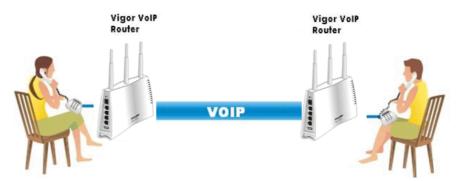


If you both register to the same SIP Registrar, then it will be illustrated as below:

The major benefit of this mode is that you don't have to memorize your friend's IP address, which might change very frequently if it's dynamic. Instead of that, you will only have to using **dial plan** or directly dial your friend's **account name** if you are with the same SIP Registrar.

Peer-to-Peer

Before calling, you have to know your friend's IP Address. The Vigor VoIP Routers will build connection between each other.



Our Vigor V models firstly apply efficient codecs designed to make the best use of available bandwidth, but Vigor V models also equip with automatic QoS assurance. QoS Assurance assists to assign high priority to voice traffic via Internet. You will always have the required inbound and outbound bandwidth that is prioritized exclusively for Voice traffic over Internet but you just get your data a little slower and it is tolerable for data traffic.



3.5.1 DialPlan

This page allows you to set phone book and digit map for the VoIP function. Click the **Phone Book** and **Digit Map** links on the page to access into next pages for dialplan settings.

VoIP >> DialPlan Se	up
DialPlan Configuratio	n
	Phone Book
	<u>Digit Map</u>
	Call Barring
	Regional
	PSTN Setup

Phone Book

In this section, you can set your VoIP contacts in the "phonebook". It can help you to make calls quickly and easily by using "speed-dial" **Phone Number**. There are total 60 index entries in the phonebook for you to store all your friends and family members' SIP addresses. **Loop through** and **Backup Phone Number** will be displayed if you are using Vigor2110Vn for setting the phone book.



VoIP >> DialPlan Setup

Index	Phone number	Display Name	SIP URL	Dial Out Account	Loop through	Backup Phone Number	Status
<u>1.</u>				Default	None		×
<u>2.</u>				Default	None		×
<u>3.</u>				Default	None		×
<u>4.</u>				Default	None		×
<u>5.</u>				Default	None		×
<u>6.</u>				Default	None		×
<u>7.</u>				Default	None		×
<u>8.</u>				Default	None		×
<u>9.</u>				Default	None		×
<u>10.</u>				Default	None		×
<u>11.</u>				Default	None		×
<u>12.</u>				Default	None		×
<u>13.</u>				Default	None		×
<u>14.</u>				Default	None		×
<u>15.</u>				Default	None		×
<u>16.</u>				Default	None		×
<u>17.</u>				Default	None		×
<u>18.</u>				Default	None		×
<u>19.</u>				Default	None		×
<u>20.</u>				Default	None		×

Status: v --- Active, x --- Inactive, ? --- Empty

Click any index number to display the dial plan setup page.

Phone Book I			
	Phone Number	1	
	Display Name	Polly	
	SIP URL	1112	
	Dial Out Account	Default 🚩	
	Loop through	None 💌	
	Backup Phone Number]
	OK	Clear (Cancel

VoIP >> DialPlan Setup

Enable	Click this to enable this entry.		
Phone Number	The speed-dial number of this index. This can be any number you choose, using digits 0-9 and * .		
Display Name	The Caller-ID that you want to be displayed on your friend's screen. This let your friend can easily know who's calling without memorizing lots of SIP URL Address.		
SIP URL	Enter your friend's SIP Address.		
Dial Out Account	Choose one of the SIP accounts for this profile to dial out. It is useful for both sides (caller and callee) that registered to different SIP Registrar servers. If caller and callee do not use		

Dray Tek

	the same SIP server, sometimes, the VoIP phone call connection may not succeed. By using the specified dial out account, the successful connection can be assured.		
Loop through	The selection should be as the following:		
	Loop through	None 🔽	
	Backup Phone Number	None PSTN	
Backup Phone Number	Backun Phone Number		

Dray Tek

Digit Map

For the convenience of user, this page allows users to edit prefix number for the SIP account with adding number, stripping number or replacing number. It is used to help user having a quick and easy way to dial out through VoIP interface.

Dig	it Map S	letup					
#	Enable	Prefix Number	Mode	OP Number	Min Len	Max Len	Interface
1	✓	03	Replace 🔽	8863	7	9	PSTN 🔽
2	✓	886	Strip 🔽	886	8	10	PSTN 🔽
З			None 🔽		0	0	PSTN 🗸
4			None 🔽		0	0	PSTN 🔽
5			None 🔽		0	0	PSTN 🔽
6			None 🔽		0	0	PSTN 🔽
7			None 🗸		0	0	PSTN 🔽
8			None 🔽		0	0	PSTN 🔽
9			None 🔽		0	0	PSTN 🔽
10			None 🔽		0	0	PSTN 🔽
11			None 🔽		0	0	PSTN 🔽
12			None 🔽		0	0	PSTN 🔽
13			None 🔽		0	0	PSTN 🔽
14			None 🔽		0	0	PSTN 🔽
15			None 🔽		0	0	PSTN 🔽
16			None 🔽		0	0	PSTN 🔽
17			None 🔽		0	0	PSTN 🔽
18			None 🔽		0	0	PSTN 🔽
19			None 🔽		0	0	PSTN 🔽
20			None 🔽		0	0	PSTN 🔽

VoIP >> DialPlan Setup

Note: Min Len and Max Len should be between 0~25.

Enable	Check this box to invoke this setting.
Prefix Number	The phone number set here is used to add, strip, or replace the OP number.
Mode	 None - No action. Add - When you choose this mode, the OP number will be added with the prefix number for calling out through the specific VoIP interface. Strip - When you choose this mode, the OP number will be deleted by the prefix number for calling out through the specific VoIP interface. Take the above picture (Prefix Table Setup web page) as an example, the OP number of <i>886</i> will be deleted completely for the prefix number is set with <i>886</i>. Replace - When you choose this mode, the OP number will be replaced by the prefix number for calling out through the

Cancel

ОK

specific VoIP interface. Take the above picture (Prefix Table Setup web page) as an example, the prefix number of 03 will be replaced by 8863. For example: dial number of "031111111" will be changed to "8863111111" and sent to SIP server. Mode

Replace	*
None	
Add	
Strip	
Replace	

OP Number	The front number you type here is the first part of the account number that you want to execute special function (according to the chosen mode) by using the prefix number.	
Min Len	Set the minimal length of the dial number for applying the prefix number settings. Take the above picture (Prefix Table Setup web page) as an example, if the dial number is between 7 and 9, that number can apply the prefix number settings here.	
Max Len	Set the maximum length of the dial number for applying the prefix number settings.	
Interface	Choose the one that you want to enable the prefix number settings from the saved SIP accounts. Please set up one SIP account first to make this interface available.	

Call Barring

Call barring is used to block phone calls coming from the one that is not welcomed.

Call Barr	ing Setup			Set to Factor	<u>y Default</u>
Index	Call Direction	Barring Type	Barring Number/URL/URI	Interface	Status
<u>1.</u>					x
<u>2.</u>					x
<u>3.</u>					x
<u>4.</u>					x
<u>5.</u>					x
<u>6.</u>					x
<u>7.</u>					x
<u>8.</u>					x
<u>9.</u>					х
<u>10.</u>					x
<< <u>1-10</u>	<u>11-20</u> >>				Next >>

VoIP >> DialPlan Setup

.....

Advanced: Block Anonymous Block Unknown Domain Block IP Address



Click any index number to display the dial plan setup page.

VolP >> DialPlan Setup

VoIP >> DialPlan Setup

Call Barring Index No. 1			
Enable			
Call Direction	IN 💌		
Barring Type	Specific URI/URL 💌		
Specific URI/URL			
Interface	All 🖌		
	OK Cancel		
Enable	Click this to enable this entry.		
Call Direction	Determine the direction for the phone call, IN – incoming call, OUT-outgoing call, IN & OUT – both incoming and outgoing calls.		
Barring Type	Determine the type of the VoIP phone call, URI/URL or number. Specific URI/URL Specific URI/URL Specific Number		
Specific URI/URL or Specific Number	This field will be changed based on the type you selected for barring Type.		
Interface	All means all the phone calls will be blocked with such mechanism.		
	lvanced settings for call barring such as Block Anonymous , Block k IP Address . Simply click the relational links to open the web		

For **Block Anonymous** – this function can block the incoming calls without caller ID on the interface (Phone port) specified in the following window.

Call Barring Block Anonymous	5	
🗹 Enable		
Interface	Phone1	Phone2
Note:Block the incoming calls w	hich do not hav	ve the caller ID.

Cancel



0K

For **Block Unknown Domain** – this function can block incoming calls (through Phone port) from unrecognized domain that is not specified in SIP accounts.

VoIP >> DialPlan Setup

Call Barring Block Unknown Domain	
Enable	
Interface 🗌 Phone1	Phone2
Note:If the domain of the incoming call is different should be blocked.	erent from the domain found in SIP accounts, the call
O	K Cancel

For **Block IP Address** – this function can block incoming calls (through Phone port) coming from IP address.

VoIP >> Dia	alPlan Setup		
Call Barring	g Block IP Address		
🗹 Enable			
1	Interface	Phone1	Phone2
Note:The in	coming calls by means	of IP dialing	(e.g.#192*168*1*1#) should be blocked.
		OK	Cancel

Regional

This page allows you to process incoming or outgoing phone calls by regional. Default values (common used in most areas) will be shown on this web page. You *can change* the number based on the region that the router is placed.

Enable Regional			1	Set to Fac	tory Default
Last Call Return [Miss]:	*69]			
Last Call Return [In]:	*12]	Last Call Return [Out]:	*14	
Call Forward [All] [Act]:	*72	+number+#	Call Forward [Deact]:	*73	+#
Call Forward [Busy] [Act]:	*90	+number+#	Call Forward [No Ans] [Act]:	*92	+number+#
Do Not Disturb [Act]:	*78	+#	Do Not Disturb [Deact]:	*79	+#
Hide caller ID [Act]:	*67	+#	Hide caller ID [Deact]:	*68	+#
Call Waiting [Act]:	*56	+#	Call Waiting [Deact]:	*57	+#
Block Anonymous [Act]:	*77	+#	Block Anonymous [Deact]:	*87	+#
Block Unknow Domain [Act]:	*40	+#	Block Unknow Domain [Deact]:	*04	+#
Block IP Calls [Act]:	*50	+#	Block IP Calls [Deact]:	*05	+#
Block Last Calls [Act]:	*60	+#			
		ОК	Cancel		

VoIP >> DialPlan Setup



Last Call Return [Miss]	Sometimes, people might miss some phone calls. Please dial number typed in this field to know where the last phone call comes from and call back to that one.
Last Call Return [In]	You have finished an incoming phone call, however you want to call back again for some reason. Please dial number typed in this field to call back to that one.
Last Call Return [Out]	Dial the number typed in this field to call the previous outgoing phone call again.
Call Forward [All][Act]	Dial the number typed in this field to forward all the incoming calls to the specified place.
Call Forward [Deact]	Dial the number typed in this field to release the call forward function.
Call Forward [Busy][Act]	Dial the number typed in this field to forward all the incoming calls to the specified place while the phone is busy.
Call Forward [No Ans][Act] Dial the number typed in this field to forward all the incoming calls to the specified place while there is no answer of the connected phone.
Do Not Disturb [Act]	Dial the number typed in this field to invoke the function of DND.
Do Not Distrub [Deact]	Dial the number typed in this field to release the DND function.
Hide caller ID [Act]	Dial the number typed in this field to make your phone number (ID) not displayed on the display panel of remote end.
Hide caller ID [Deact]	Dial the number typed in this field to release this function.
Call Waiting [Act]	Dial the number typed in this field to make all the incoming calls waiting for your answer.
Call Waiting [Deact]	Dial the number typed in this field to release this function.
Block Anonymous[Act]	Dial the number typed in this field to block all the incoming calls with unknown ID.
Block Anonymous[Deact]	Dial the number typed in this field to release this function.
Block Unknown Domain [Act]	Dial the number typed in this field to block all the incoming calls from unknown domain.
Block Unknown Domain [Deact]	Dial the number typed in this field to release this function.
Block IP Calls [Act]	Dial the number typed in this field to block all the incoming calls from IP address.
Block IP Calls [Deact]	Dial the number typed in this field to release this function.

Block Last Calls [Act]

Dial the number typed in this field to block the last incoming phone call.

PSTN Setup

Some emergency phone (e.g., 911) or special phone cannot be dialed out by using VoIP and can be called out through PSTN line only. To solve this problem, this page allows you to set five sets of PSTN number for dialing without passing through Internet. Please type the number in the field of **phone number for PSTN relay**.

VAIDSS	DOTM	Cature
VoIP >>	F 3 1 N	Setub

Enable	phone number for PSTN relay

Then, check the **Enable** box to make the PSTN number available for dial whenever you need.

3.5.2 SIP Accounts

In this section, you set up your own SIP settings. When you apply for an account, your SIP service provider will give you an **Account Name** or user name, **SIP Registrar, Proxy,** and **Domain name**. (The last three might be the same in some case). Then you can tell your folks your SIP Address as in **Account Name@ Domain name**

As Vigor VoIP Router is turned on, it will first register with Registrar using AuthorizationUser@Domain/Realm. After that, your call will be bypassed by SIP Proxy to the destination using AccountName@Domain/Realm as identity.

SIP Acc	ounts Lis	t				ſ	Refresh
Index	Profile	Domain/Realm	Proxy	Account Name	Ring	ے Port	Status
1					Phone1	Phone2	-
<u>2</u>					Phone1	Phone2	-
<u>3</u>					Phone1	Phone2	-
4					Phone1	Phone2	-
<u>5</u>					Phone1	Phone2	-
<u>6</u>					Phone1	Phone2	-
NAT Tra	versal Se	etting				egistered on 9 ster on SIP si	

STUN Server:				
External IP:]	
SIP PING Interval:	150	sec		

_		_
	OK	

Index	Click this link to access into next page for setting SIP account.
Profile	Display the profile name of the account.
Domain/Realm	Display the domain name or IP address of the SIP registrar server.
Proxy	Display the domain name or IP address of the SIP proxy server.
Account Name	Display the account name of SIP address before @.
Ring Port	Specify which port will ring when receiving a phone call.
STUN Server	Type in the IP address or domain of the STUN server.
External IP	Type in the gateway IP address.
SIP PING interval	The default value is 150 (sec). It is useful for a Nortel server NAT Traversal Support.
Status	Show the status for the corresponding SIP account. R means such account is registered on SIP server successfully. – means the account is failed to register on SIP server.

VoIP >> SIP Accounts

Profile Name	(11 char max.)
Register via	None 🕑 🔲 Call without Registration
SIP Port	5060
Domain/Realm	(63 char max.)
Proxy	(63 char max.)
Act as outbound pro	ху
Display Name	(23 char max.)
Account Number/Name	(63 char max.)
Authentication ID	(63 char max.)
Password	(63 char max.)
Expiry Time	1 hour 🕑 3600 sec
NAT Traversal Support	None 💌
Ring Port	Phone 1 Phone 2
Ring Pattern	1 💌

Profile Name	Assign a name for this profile for identifying. You can type similar name with the domain. For example, if the domain name is <i>draytel.org</i> , then you might set <i>draytel-1</i> in this field.
Register via	If you want to make VoIP call without register personal information, please choose None and check the box to achieve the goal. Some SIP server allows user to use VoIP function without registering. For such server, please check the box of Call without registration . Choosing Auto is recommended. None Auto WAN1 LAN/VPN
SIP Port	Set the port number for sending/receiving SIP message for building a session. The default value is 5060. Your peer must set the same value in his/her Registrar.
Domain/Realm	Set the domain name or IP address of the SIP Registrar server.
Proxy	Set domain name or IP address of SIP proxy server. By the time you can type :port number after the domain name to specify that port as the destination of data transmission (e.g., nat.draytel.org:5065)
Act as Outbound Proxy	Check this box to make the proxy acting as outbound proxy.
Display Name	The caller-ID that you want to be displayed on your friend's screen.
Account Number/Name	Enter your account name of SIP Address, e.g. every text before @.
Authentication ID	Check the box to invoke this function and enter the name or number used for SIP Authorization with SIP Registrar. If this



	setting value is the same as Account Name, it is not necessary for you to check the box and set any value in this field.					
Password	The password provided to you when you registered with a SIP service.					
Expiry Time	The time duration that your SIP Registrar server keeps your registration record. Before the time expires, the router will send another register request to SIP Registrar again.					
NAT Traversal Support	If the router (e.g., broadband router) you use connects to internet by other device, you have to set this function for your necessity.					
	NAT Traversal Support None None Stun Manual Nortel					
	 None – Disable this function. Stun – Choose this option if there is Stun server provided for your router. Manual – Choose this option if you want to specify an external IP address as the NAT transversal support. Nortel – If the soft-switch that you use supports Nortel solution, you can choose this option. 					
Ring Port	Set Phone1 or Phone2 as the default ring port for this SIP account.					
Ring Pattern	Choose a ring tone type for the VoIP phone call. Ring Pattern 1 2 3 4 5 6					

3.5.3 Phone Settings

This page allows user to set phone settings for Phone 1 and Phone 2 respectively. However, it changes slightly according to different model you have.

Phone	List							
Index	Port	Call Feature	Codec	Tone	Gain (Mic/Speaker)	Default SIP Account	DTMF Relay	
1	Phone1	CW,CT,	G.729A/B	User Defined	5/5		InBand	
2	Phone2	CW,CT,	G.729A/B	User Defined	5/5		InBand	
лтр								
	🗌 Syr	nmetric RTP						
Dynamic RTP Port Start			10050					
Dynamic RTP Port End				15000				
RTP TOS				IP precedence 5 🛛 🖌 10100000				

Phone List Port – there are two phone ports provided here for you to configure. Phone1/Phone2 allow you to set general settings for PSTN phones. Call Feature – A brief description for call feature will be shown in this field for your reference. **Codec** – The default Codec setting for each port will be shown in this field for your reference. You can click the number below the Index field to change it for each phone port. Tone - Display the tone settings that configured in the advanced settings page of Phone Index. Gain - Display the volume gain settings for Mic/Speaker that configured in the advanced settings page of Phone Index. **Default SIP Account** – "draytel_1" is the default SIP account. You can click the number below the Index field to change SIP account for each phone port. DTMF Relay – Display DTMF mode that configured in the advanced settings page of Phone Index. RTP Symmetric RTP – Check this box to invoke the function. To make the data transmission going through on both ends of local router and remote router not misleading due to IP lost (for example, sending data from the public IP of remote router to the private IP of local router), you can check this box to solve this problem. Dynamic RTP Port Start - Specifies the start port for RTP stream. The default value is 10050. Dynamic RTP Port End - Specifies the end port for RTP stream. The default value is 15000. **RTP TOS** – It decides the level of VoIP package. Use the drop



down list to choose any one of them.

Manual	
IP precedence 1	
IP precedence 2	
IP precedence 3	
IP precedence 4	
IP precedence 5	
IP precedence 6	
IP precedence 7	
AF Class1 (Low Drop)	
AF Class1 (Medium Drop)	
AF Class1 (High Drop)	
AF Class2 (Low Drop)	
AF Class2 (Medium Drop)	
AF Class2 (High Drop)	
AF Class3 (Low Drop)	
AF Class3 (Medium Drop)	
AF Class3 (High Drop)	
AF Class4 (Low Drop)	
AF Class4 (Medium Drop)	
AF Class4 (High Drop)	
EF Class	
Manual	~

RTP TOS

Detailed Settings for Phone Port

Click the number link for Phone port, you can access into the following page for configuring Phone settings.

VoIP >> Phone Settings

Phone1					
Call Feature			Codecs		
Hotline			Prefer Codec	G.729A/B (8Kbps)	
Session Timer	90	sec		Single Codec	
Call Forwarding	Disable 🔽		Packet Size	20ms 🕶	
SIP URL			Voice Active Detector	Off 🛩	
Time Out	30 sec		Default SIP Account	~	
DND(Do Not Disturb) Mode			Play dial tone only when account registered		
Index(1-60) in Phor	<u>ne Book</u> as Excep	tion List:		inicit debbane registered	
		,			
CLIR (hide caller ID)					
Call Waiting					
Call Transfer					
	ОК	Ca	Advanced		
Hotline			to enable it. Type in the tically when you pick	e SIP URL in the field for up the phone set.	
Session Timer	you se	t in this f	x to enable the function. In the limited time that s field, if there is no response, the connecting call l automatically.		
Call Forwarding	forwar be forw the inc the loc	ction. Always means a nto SIP URL without a alls will be forwarded n is busy. No Answer	ose. Disable is to close cal all the incoming calls will any reason. Busy means into SIP URL only when means if the incoming y will be forwarded to the		

	SIP URL by the time out. Disable Disable Always Busy No Answer SIP URL – Type in the SIP URL (e.g., aaa@draytel.org or abc@iptel.org) as the site for call forwarded. Time Out – Set the time out for the call forwarding. The default setting is 30 sec.
DND (Do Not Disturb) mode	Set a period of peace time without disturbing by VoIP phone call. During the period, the one who dial in will listen busy tone, yet the local user will not listen any ring tone.
	Index (1-60) in Phone Book - Enter the index of phone book profiles. Refer to section VoIP>>DialPlan>>Phone Book for detailed configuration.
CLIR (hide caller ID)	Check this box to hide the caller ID on the display panel of the phone set.
Call Waiting	Check this box to invoke this function. A notice sound will appear to tell the user new phone call is waiting for your response. Click hook flash to pick up the waiting phone call.
Call Transfer	Check this box to invoke this function. Click hook flash to initiate another phone call. When the phone call connection succeeds, hang up the phone. The other two sides can communicate, then.
Prefer Codec	Select one of five codecs as the default for your VoIP calls. The codec used for each call will be negotiated with the peer party before each session, and so may not be your default choice. The default codec is G.729A/B; it occupies little bandwidth while maintaining good voice quality. If your upstream speed is only 64Kbps, do not use G.711 codec. It is better for you to have at least 256Kbps upstream if you would like to use G.711.
	Prefer Codec G.711A (64Kbps) ✓ G.711MU (64Kbps) G.711A (64Kbps) G.711A (64Kbps) G.729A/B (8Kbps) G.723 (6.4kbps) G.723 (6.4kbps) G.726_32 (32kbps) G.726_32 (32kbps) G.726_32 (32kbps)
	 Single Codec – If the box is checked, only the selected Codec will be applied. Packet Size-The amount of data contained in a single packet. The default value is 20 ms, which means the data packet will contain 20 ms voice information.

Packet Size





Voice Active Detector - This function can detect if the voice on both sides is active or not. If not, the router will do something to save the bandwidth for other using. Click On to invoke this function; click off to close the function.

Voice Active Detector



Default SIP Account

You can set SIP accounts (up to six groups) on SIP Account page. Use the drop down list to choose one of the profile names for the accounts as the default one for this phone setting.

Play dial tone only when account registered - Check this box to invoke the function.

In addition, you can press the **Advanced** button to configure tone settings, volume gain, MISC and DTMF mode. **Advanced** setting is provided for fitting the telecommunication custom for the local area of the router installed. Wrong tone settings might cause inconvenience for users. To set the sound pattern of the phone set, simply choose a proper region to let the system find out the preset tone settings and caller ID type automatically. Or you can adjust tone settings manually if you choose User Defined. TOn1, TOff1, TOn2 and TOff2 mean the cadence of the tone pattern. TOn1 and TOn2 represent sound-on; TOff1 and TOff2 represent the sound-off.

Tone Se	ttings						
Region	User Defined	*		Cal	ler ID Type	FSK_ETSI	~
		Low Freq (Hz)	High Freq (Hz)	T on 1 (msec)	T off 1 (msec)	T on 2 (msec)	T off 2 (msec)
Dia	al tone	350	440	0	0	0	0
Ring	ing tone	400	450	400	200	400	2000
Bus	sy tone	400	0	375	375	0	0
Conge	stion tone	0	0	0	0	0	0
Volume	Gain			DTMF			
Mic Gain	(1-10)	5		DTMF Mod	le	InBand	~
Speaker Gain(1-10) 5 Payload Type(RFC2833) 101							
MISC							
Dial Tone	e Power Level	l (1 - 50) 2	7				
Ring Fred	quency (10 -	50HZ) 25	5				

VoIP >> Phone Settings

Region

Select the proper region which you are located. The common settings of **Caller ID Type**, **Dial tone**, **Ringing tone**, **Busy tone** and **Congestion tone** will be shown automatically on the page. If you cannot find out a suitable one, please choose **User Defined** and fill out the corresponding values for dial tone, ringing tone, busy tone, congestion tone by yourself for VoIP phone.

	mu v anteo v	and the second s	r manne	
	Tone Set	tings		
	Region	User Defined	ow	
	Dia	UK US Denmark	(H O	
	Ringi	ltaly Germany Netherlands	0	
	Conge	Dortugal		
	Volume	Australia		
	Mic Gain(Czech		
	Speaker MISC	Slovakia Hungary Switzerland		
	Dial Tone	Power Level	(1 - 50	
	-	l for you to use	ield for your necessi the default settings	-
Volume Gain	microphone a	nd speaker by o	ain (1-10) - Adjust entering number from der the volume is.	
MISC	loudness of th the dial tone is setting. Ring Frequen	e dial tone. Th s. It is recomm ncy - This setti	nis setting is used to e smaller the numbe ended for you to use ng is used to drive the ided for you to use the	er is, the louder the default he frequency of
DTMF	<i>InBand</i> - Cho tone as audio <i>OutBand</i> - Ch	oose this one th directly when noose this one t	our DTMF modes for en the Vigor will ser you press the keypac then the Vigor will c	nd the DTMF l on the phone capture the
			and transform it to c	
			he receiver will gene it receive. This fund	
			fic congestion occur	
		e accuracy of I	<u> </u>	
			then the Vigor will	
			to SIP form. Then i	t will be sent to
		d with SIP mes		
	DTMF mode		InBand	×
			InBand OutBand (RFC2833	3)
			SIP INFO (cisco for	
			SIP INFO (nortel for	

Payload Type (rfc2833) - Choose a number from 96 to 127, the default value was 101. This setting is available for the OutBand (RFC2833) mode.



3.5.4 Status

From this page, you can find codec, connection and other important call status for each port.

Vol	P >>	Stati	JS
-----	------	-------	----

Status								Refresł	n Seco	nds:	10 💌	Refresh
Port	Status	Codec	PeerID	Elapse (hh:mm:ss)	Tx Pkts	Rx Pkts	Rx Losts	Rx Jitter (ms)	In Calls	Out Calls		Speaker Gain
Phone1	IDLE			00:00:00	0	0	0	0	0	0	0	5
Phone2	IDLE			00:00:00	0	0	0	0	0	0	0	5
Log Date		Time		Duration	т	n/0v+	/Miss	100	ount	TD	Peer	
(mm-dd-y	0001	(hh:m	n•aa)	(hh:mm:s:		n/ Out	/ 1135	ACC	ounc .	10	FEEL	10
00-00-	, , , , , , , , , , , , , , , , , , ,	00:00		00:00:00				_				
00-00-	0	00:00	:00	00:00:00	-			_				
00-00-	0	00:00	:00	00:00:00	-			-				
00-00-	0	00:00	:00	00:00:00	-			-				
00-00-	0	00:00	:00	00:00:00	-			-				
00-00-	0	00:00		00:00:00	-			-				
00-00-	0	00:00		00:00:00	-			-				
00-00-	0	00:00		00:00:00	-			-				
00-00-	0	00:00		00:00:00	-			-				
00-00-	0	00:00	:00	00:00:00	-			-				

Refresh Seconds

Specify the interval of refresh time to obtain the latest VoIP calling information. The information will update immediately when the Refresh button is clicked.



Port	It shows current connection status for the port of Phone1 and Phone2.
Status	It shows the VoIP connection status. IDLE - Indicates that the VoIP function is idle. HANG_UP - Indicates that the connection is not established (busy tone). CONNECTING - Indicates that the user is calling out. WAIT_ANS - Indicates that a connection is launched and waiting for remote user's answer. ALERTING - Indicates that a call is coming. ACTIVE-Indicates that the VoIP connection is launched.
Codec	Indicates the voice codec employed by present channel.
PeerID	The present in-call or out-call peer ID (the format may be IP or Domain).

Rx PktsTotal number of received voice packets during this connection
session.



Elapse

Rx Losts	Total number of lost packets during this connection session.
Rx Jitter	The jitter of received voice packets.
In Calls	Accumulation for the times of in call.
Out Calls	Accumulation for the times of out call.
Miss Calls	Accumulation for the times of missing call.
Speaker Gain	The volume of present call.
Log	Display logs of VoIP calls.

3.6 Wireless LAN

This function is used for "n" models.

3.6.1 Basic Concepts

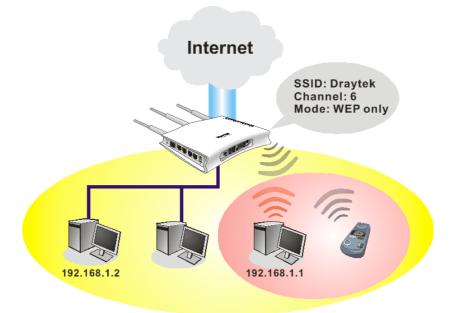
Over recent years, the market for wireless communications has enjoyed tremendous growth. Wireless technology now reaches or is capable of reaching virtually every location on the surface of the earth. Hundreds of millions of people exchange information every day via wireless communication products. The Vigor "n" model, a.k.a. Vigor wireless router, is designed for maximum flexibility and efficiency of a small office/home. Any authorized staff can bring a built-in WLAN client PDA or notebook into a meeting room for conference without laying a clot of LAN cable or drilling holes everywhere. Wireless LAN enables high mobility so WLAN users can simultaneously access all LAN facilities just like on a wired LAN as well as Internet access

The Vigor wireless routers are equipped with a wireless LAN interface compliant with the standard IEEE 802.11n draft 2 protocol. To boost its performance further, the Vigor Router is also loaded with advanced wireless technology to lift up data rate up to 300 Mbps*. Hence, you can finally smoothly enjoy stream music and video.

Note: * The actual data throughput will vary according to the network conditions and environmental factors, including volume of network traffic, network overhead and building materials.

In an Infrastructure Mode of wireless network, Vigor wireless router plays a role as an Access Point (AP) connecting to lots of wireless clients or Stations (STA). All the STAs will share the same Internet connection via Vigor wireless router. The **General Settings** will set up the information of this wireless network, including its SSID as identification, located channel etc.





Security Overview

Real-time Hardware Encryption: Vigor Router is equipped with a hardware AES encryption engine so it can apply the highest protection to your data without influencing user experience.

Complete Security Standard Selection: To ensure the security and privacy of your wireless communication, we provide several prevailing standards on market.

WEP (Wired Equivalent Privacy) is a legacy method to encrypt each frame transmitted via radio using either a 64-bit or 128-bit key. Usually access point will preset a set of four keys and it will communicate with each station using only one out of the four keys.

WPA (Wi-Fi Protected Access), the most dominating security mechanism in industry, is separated into two categories: WPA-personal or called WPA Pre-Share Key (WPA/PSK), and WPA-Enterprise or called WPA/802.1x.

In WPA-Personal, a pre-defined key is used for encryption during data transmission. WPA applies Temporal Key Integrity Protocol (TKIP) for data encryption while WPA2 applies AES. The WPA-Enterprise combines not only encryption but also authentication.

Since WEP has been proved vulnerable, you may consider using WPA for the most secure connection. You should select the appropriate security mechanism according to your needs. No matter which security suite you select, they all will enhance the over-the-air data protection and /or privacy on your wireless network. The Vigor wireless router is very flexible and can support multiple secure connections with both WEP and WPA at the same time.

Separate the Wireless and the Wired LAN- WLAN Isolation enables you to isolate your wireless LAN from wired LAN for either quarantine or limit access reasons. To isolate means neither of the parties can access each other. To elaborate an example for business use, you may set up a wireless LAN for visitors only so they can connect to Internet without hassle of the confidential information leakage. For a more flexible deployment, you may add filters of MAC addresses to isolate users' access from wired LAN.

Manage Wireless Stations - Station List will display all the station in your wireless network and the status of their connection.

Below shows the menu items for Wireless LAN.



Wireless LAN

3.6.2 General Setup

By clicking the **General Settings**, a new web page will appear so that you could configure the SSID and the wireless channel. Please refer to the following figure for more information.

Wireless LAN >> General Setup

Enable Wireless LAN	
Mode :	Mixed(11b+11g+11n)
SSID:	DrayTek
Channel :	Channel 6, 2437MHz 💌
Packet-OVERDRIVE TM	
Tx Burst	
Note:	
The same technology mus	at also be supported in clients to boost WLAN performance.
Hide SSID	
Long Preamble	
Hide SSID: prevent SSID Long Preamble: necessa	from being scanned. ary for some older 802.11b devices only (lowers performance).
	OK Cancel
ble Wireless LAN	Check the box to enable wireless function.
le	At present, the router can connect to Mixed (11b+11g)
	11g Only, 11b Only, Mixed (11g+11n), 11n Only and
	Mixed (11b+11g+11n) stations simultaneously. Simply
	choose Mix (11b+11g+11n) mode.
	Mixed(11b+11g+11n)
	11b Only
	11g Only

Mixed(11g+11n)Mixed(11b+11g+11n)SSIDMeans the identification of the wireless LAN. SSID can be
any text numbers or various special characters. The default
SSID is "DrayTek". We suggest you to change it.ChannelMeans the channel of frequency of the wireless LAN. The
default channel is 6. You may switch channel if the
selected channel is under serious interference. If you have
no idea of choosing the frequency, please select Auto to let
system determine for you.



11n Only Mixed(11b+11g)

Channel:	Channel 6, 2437MHz 🛛 💌	
	Auto	
	Channel 1, 2412MHz	
	Channel 2, 2417MHz	
	Channel 3, 2422MHz	
	Channel 4, 2427MHz	
	Channel 5, 2432MHz	
	Channel 6, 2437MHz	
	Channel 7, 2442MHz	
	Channel 8, 2447MHz	
	Channel 9, 2452MHz	
	Channel 10, 2457MHz	
	Channel 11, 2462MHz	
	Channel 12, 2467MHz	
	Channel 13, 2472MHz	

Packet-OVERDRIVE

This feature can enhance the performance in data transmission about 40% * more (by checking **Tx Burst**). It is active only when both sides of Access Point and Station (in wireless client) invoke this function at the same time. That is, the wireless client must support this feature and invoke the function, too.

Note: Vigor N61 wireless adapter supports this function. Therefore, you can use and install it into your PC for matching with Packet-OVERDRIVE (refer to the following picture of Vigor N61 wireless utility window, choose **Enable** for **TxBURST** on the tab of **Option**).

Vigor N61 802.11n Wireless USB Adapter Utility			×
Configuration Status Option About			
General Setting Auto launch when Windows gtart up Remember mini status position Auto hide mini status Set mini status always on top Enable IP Setting and Proxy Setting in Profile Group Reaming Albane	Advance Setting Disable <u>R</u> adio <u>Fragmentation Threshold</u> : RTS Thresh <u>old</u> : Frequency: Ad-hoc <u>Channel</u> : Power Save Mode:	2346 2347 802.11b/g/n - 2.40H ¥ 1 ¥	
Group Koanmig Ad-hoc	Tx <u>B</u> urst :	Disable V	
WLAN type to connect Unfrastructure and Ad-hoc getwork Infrastructurg network only Ad-hoc network only Automatically connect to non-preferred networks			
	OK (Cancel Apply	7

Hide SSID
 Check it to prevent from wireless sniffing and make it harder for unauthorized clients or STAs to join your wireless LAN. Depending on the wireless utility, the user may only see the information except SSID or just cannot see any thing about Vigor wireless router while site surveying. The system allows you to set four sets of SSID for different usage. In default, the first set of SSID will be enabled. You can hide it for your necessity.
 Long Preamble
 This option is to define the length of the sync field in an 802.11 packet. Most modern wireless network uses short

This option is to define the length of the sync field in an 802.11 packet. Most modern wireless network uses short preamble with 56 bit sync field instead of long preamble



with 128 bit sync field. However, some original 11b wireless network devices only support long preamble. Check it to use Long Preamble if needed to communicate with this kind of devices.

3.6.3 Security

By clicking the Security Settings, a new web page will appear so that you could configure the settings of WEP and WPA.

Wireless	LAN >>	Security	Settings
----------	--------	----------	----------

Mode:	Disable 🗸
WPA:	
Encryption Mode:	TKIP for WPA/AES for WPA2
Pre-Shared Key(PSK):	****
Type 8~63 ASCII chara "cfgs01a2" or "0x655	acter or 64 Hexadecimal digits leading by "0x", for example abcd".
WEP:	
Encryption Mode:	64-Bit 🗸
● Key 1 :	***
○Key 2 :	****
○Key 3 :	***
○Key 4 :	***
"0x4142333132". For 128 bit WEP key	Hexadecimal digits leading by "0x", for example "AB312" or 6 Hexadecimal digits leading by "0x", for example 233343536373839414243".
	OK Cancel There are several modes provided for you to ch

N



Disable - Turn off the encryption mechanism. **WEP-**Accepts only WEP clients and the encryption key should be entered in WEP Key.

WPA/PSK-Accepts only WPA clients and the encryption key should be entered in PSK.

WPA2/PSK-Accepts only WPA2 clients and the encryption key should be entered in PSK.

Mixed (WPA+ WPA2)/PSK - Accepts WPA and WPA2 clients simultaneously and the encryption key should be entered in PSK.

WPA

The WPA encrypts each frame transmitted from the radio using the key, which either PSK (Pre-Shared Key) entered



manually in this field below or automatically negotiated via 802.1x authentication. Either **8~63** ASCII characters, such as 012345678(or 64 Hexadecimal digits leading by 0x, such as "0x321253abcde...").

Type - Select from Mixed (WPA+WPA2) or WPA2 only. **Pre-Shared Key (PSK)** - Either **8~63** ASCII characters, such as 012345678..(or 64 Hexadecimal digits leading by 0x, such as "0x321253abcde...").

64-Bit - For 64 bits WEP key, either **5** ASCII characters, such as 12345 (or 10 hexadecimal digitals leading by 0x, such as 0x4142434445.)

128-Bit - For 128 bits WEP key, either **13** ASCII characters, such as ABCDEFGHIJKLM (or 26 hexadecimal digits leading by 0x, such as 0x4142434445464748494A4B4C4D).

Encryption Mode:

	64-Bit	*
	64-Bit	
	128-Bit	
่่	a como U	

All wireless devices must support the same WEP encryption bit size and have the same key. **Four keys** can be entered here, but only one key can be selected at a time. The keys can be entered in ASCII or Hexadecimal. Check the key you wish to use.

3.6.4 Access Control

WEP

For additional security of wireless access, the **Access Control** facility allows you to restrict the network access right by controlling the wireless LAN MAC address of client. Only the valid MAC address that has been configured can access the wireless LAN interface. By clicking the **Access Control**, a new web page will appear, as depicted below, so that you could edit the clients' MAC addresses to control their access rights.

Wireless LAN >> Access Control

I FUODIO MOOI	ess Control	
	Policy :	Activate MAC address filter 💌
		MAC Address Filter
	Index Attribut	te MAC Address
	Client's MAC .	Address :
		Attribute :
		s: Isolate the station from LAN
	1	S: Isolate the station from LAN

Enable Access Control

Select to enable the MAC Address access control feature.



Policy	Select to enable any one of the following policy. Choose Activate MAC address filter to type in the MAC addresses for other clients in the network manually. Choose Isolate WLAN from LAN will separate all the WLAN stations from LAN based on the MAC Address list. Policy : Activate MAC address filter Activate MAC address filter Isolate WLAN from LAN		
MAC Address Filter	Display all MAC addresses that are edited before.		
Client's MAC Address	Manually enter the MAC address of wireless client.		
Attribute	s: Isolate the station from LAN - select to isolate the wireless connection of the wireless client of the MAC address from LAN.		
Add	Add a new MAC address into the list.		
Delete	Delete the selected MAC address in the list.		
Edit	Edit the selected MAC address in the list.		
Cancel	Give up the access control set up.		
ОК	Click it to save the access control list.		
Clear All Clean all entries in th	e MAC address list.		

Dray Tek

3.6.5 Station List

Station List provides the knowledge of connecting wireless clients now along with its status code. There is a code summary below for explanation. For convenient Access Control, you can select a WLAN station and click Add to Access Control below.

	Status	MAC Address	Associated with
		Refresh	
	C: Connected, E: Connected, P: Connected, A: Connected, B: Blocked by A N: Connecting. F: Fail to pass	WEP. WPA. WPA2.	
			ter successfully, it may be will still be on the list until the
	Add to <u>Access</u>	Control :	
	Client's MAC ad	dress :::::	: :
		Add]
efresh		Click this b	utton to refresh the status of statio

Wireless LAN >> Station List

Click this button to refresh the status of station list.

Add

Click this button to add current typed MAC address into Access Control.

3.7 System Maintenance

For the system setup, there are several items that you have to know the way of configuration: Status, Administrator Password, Configuration Backup, Syslog, Time setup, Reboot System, Firmware Upgrade.

Below shows the menu items for System Maintenance.

System Maintenance



3.7.1 System Status

The **System Status** provides basic network settings of Vigor router. It includes LAN and WAN interface information. Also, you could get the current running firmware version or firmware related information from this presentation.

System Status

Model Name Firmware Vers Build Date/Tim		: Vigor2110 : 3.3.1 : Jul 29 200			
		LAN			WAN 1
MAC Addre	SS	: 00-50-7	F-9A-32-70	Link Status	: Connected
1st IP Addr	ress	: 192.168.	1.1	MAC Address	: 00-50-7F-9A-32-71
1st Subnet	Mask	: 255.255.	.255.0	Connection	: DHCP Client
DHCP Serve	er	: Yes		IP Address	: 192.168.5.29
DNS		: 168.95.1	.1	Default Gateway	: 192.168.5.1
		VoIP		Wi	reless LAN
Port	Profile	Reg.	In/Out	MAC Address	: 00-50-7F-9A-32-70
Phone1		No	0/0	Frequency Domain	: Europe
Phone2		No	0/0	Firmware Version	: 1.8.1.0
				SSID	: DrayTek

Model Name	Display the model name of the router.
Firmware Version	Display the firmware version of the router.
Build Date/Time	Display the date and time of the current firmware build.
LAN	
MAC Address	Display the MAC address of the LAN Interface.
1 st IP Address	Display the IP address of the LAN interface.
1 st Subnet Mask	Display the subnet mask address of the LAN interface.
DHCP Server	Display the current status of DHCP server of the LAN interface.
DNS	Display the assigned IP address of the primary DNS.
WAN	
Link Status	Display current connection status.
MAC Address	Display the MAC address of the WAN Interface.
Connection	Display the connection type.
IP Address	Display the IP address of the WAN interface.
Default Gateway	Display the assigned IP address of the default gateway.
Wireless LAN	
MAC Address	Display the MAC address of the wireless LAN.
Frequency Domain	It can be Europe (13 usable channels), USA (11 usable channels) etc. The available channels supported by the wireless products in different countries are various.
Firmware Version	It indicates information about equipped WLAN miniPCi card. This also helps to provide availability of some features that are bound with some WLAN miniPCi.



Display the SSID of the router.

3.7.2 User Password

SSID

This page allows you to set new password for user operation.

System Mainter	nance >> User Pass	word
User Password		
	Old Password	
	New Password	
	Confirm Password	
		ОК
Old Password		Type in the old password. The factory default settin

password is blank.

New Password Type in new password in this field.

Confirm Password

Type in the new password again.

When you click OK, the login window will appear. Please use the new password to access into the web configurator again.

3.7.3 Time and Date

It allows you to specify where the time of the router should be inquired from.

System Maintenance >> Tim	e and Date
Time Information	
Current System Time	2009 Mar 27 Fri 8 : 32 : 8 Inquire Time
Time Setup	
🔘 Use Browser Time	
Ose Internet Time C	lient
Server IP Address	pool.ntp.org
Time Zone	(GMT) Greenwich Mean Time : Dublin
Enable Daylight Savin	ig 🔲
Automatically Update	Interval 30 min 🛩
	OK Cancel
Current System Time	Click Inquire Time to get the current time.
Use Browser Time	Select this option to use the browser time from the remote administrator PC host as router's system time.
Use Internet Time	Select to inquire time information from Time Server on the Internet using assigned protocol.
Time Protocol	Select a time protocol.
Server IP Address	Type the IP address of the time server.
Time Zone	Select the time zone where the router is located.



for

Enable Daylight Saving	Check the box to activate daylight saving function. Such
	feature is useful for some areas.

Automatically Update Interval Select a time interval for updating from the NTP server.

Click **OK** to save these settings.

3.7.4 Reboot System

The Web Configurator may be used to restart your router for using current configuration. Click **Reboot System** from **System Maintenance** to open the following page.

System Maintenance >> Reboot System				
Reboot System	Reboot System			
	Do you want to reboot your router ?			
	Osing current configuration			
<u> </u>	OK			

Click **OK**. The router will take 5 seconds to reboot the system.

Note: When the system pops up Reboot System web page after you configure web settings, please click **OK** to reboot your router for ensuring normal operation and preventing unexpected errors of the router in the future.



3.8 Diagnostics

Diagnostic Tools provide a useful way to **view** or **diagnose** the status of your Vigor router. Below shows the menu items for Diagnostics.



3.8.1 DHCP Table

The facility provides information on IP address assignments. This information is helpful in diagnosing network problems, such as IP address conflicts, etc.

Click **Diagnostics** and click **DHCP Table** to open the web page.

Diagnostics >> View DHCP Assigned IP Addresses

HCP se	erver: Running				
Index	IP Address	MAC Address	Leased Time	HOST ID	l
L	192.168.1.12	00-1D-4F-D5-C1-39	4:16:43.820	iPod-3	

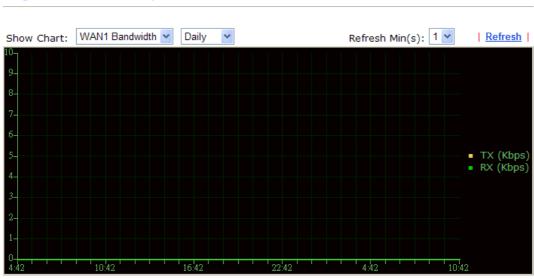
Index	It displays the connection item number.
IP Address	It displays the IP address assigned by this router for specified PC.
MAC Address	It displays the MAC address for the specified PC that DHCP assigned IP address for it.
Leased Time	It displays the leased time of the specified PC.
HOST ID	It displays the host ID name of the specified PC.
Refresh	Click it to reload the page.

Dray Tek

3.8.2 Traffic Graph

Diagnostics >> Traffic Graph

Click **Diagnostics** and click **Traffic Graph** to pen the web page. Choose WAN1 Bandwidth, Sessions, daily or weekly for viewing different traffic graph. Click **Refresh** to renew the graph at any time.



3.8.3 Ping Diagnosis

Click **Diagnostics** and click **Ping Diagnosis** to pen the web page. Diagnostics >> Ping Diagnosis

	o ping a LAN PC or you don't through, please select "Unsp	
Ping to: Host / IF	P 🝸 IP Address:	
	Run	
Result		<u>Clear</u>
		~
		× .

Ping to	Use the drop down list to choose the destination that you want to ping.
IP Address	Type in the IP address of the Host/IP that you want to ping.
Run	Click this button to start the ping work. The result will be displayed on the screen.
Clear	Click this link to remove the result on the window.

3.8.4 Trace Route

Click **Diagnostics** and click **Trace Route** to open the web page. This page allows you to trace the routes from router to the host. Simply type the IP address of the host in the box and click **Run**. The result of route trace will be shown on the screen.

Diagnostics >> Tr	ace Route	
Trace Route		
Pro	otocol:	
Ho	st / IP Address:	Run
Re	sult	<u>Clear</u>
		 ~

Protocol	Use the drop down list to choose the interface that you want to ping through.
Host/IP Address	It indicates the IP address of the host.
Run	Click this button to start route tracing work.
Clear	Click this link to remove the result on the window.

Dray Tek

4 Admin Mode Operation

This chapter will guide users to execute advanced (full) configuration through admin mode operation. As for other examples of application, please refer to chapter 5.

- 1. Open a web browser on your PC and type http://192.168.1.1. The window will ask for typing username and password.
- 2. Please type "admin/admin" on Username/Password for administration operation.

Now, the **Main Screen** will appear. Be aware that "Admin mode" will be displayed on the bottom left side.

Logout 🗸	System Status			
Status et Access	Model Name Firmware Version Build Date/Time	: Vigor2110 series : 3.3.1 : Jul 29 2009 17:05:31		
		LAN		WAN 1
are Acceleration II s Setting	MAC Address 1st IP Address 1st Subnet Mask DHCP Server DNS	: 00-50-7F-9A-32-70 : 192.168.1.1 : 255.255.255.0 : Yes : 168.95.1.1	Link Status MAC Address Connection IP Address Default Gateway	: Connected : 00-50-7F-9A-32-71 : DHCP Client : 192.168.5.29 : 192.168.5.1
ridth Management		VoIP	Wir	eless LAN
nd Remote Access cate Management	Port Profile Phone1 Phone2		MAC Address Frequency Domain Firmware Version SSID	: 00-50-7F-9A-32-70 : Europe : 1.8.1.0 : DrayTek
ss LAN Maintenance ostics			-	· ·

4.1 Internet Access

Quick Start Wizard offers user an easy method to quick setup the connection mode for the router. Moreover, if you want to adjust more settings for different WAN modes, please go to **Internet Access** group.

4.1.1 Basics of Internet Protocol (IP) Network

IP means Internet Protocol. Every device in an IP-based Network including routers, print server, and host PCs, needs an IP address to identify its location on the network. To avoid address conflicts, IP addresses are publicly registered with the Network Information Centre (NIC). Having a unique IP address is mandatory for those devices participated in the public network but not in the private TCP/IP local area networks (LANs), such as host PCs under the management of a router since they do not need to be accessed by the public. Hence, the NIC has reserved certain addresses that will never be registered publicly. These are known as *private* IP addresses, and are listed in the following ranges:



From 10.0.0.0 to 10.255.255.255 From 172.16.0.0 to 172.31.255.255 From 192.168.0.0 to 192.168.255.255

What are Public IP Address and Private IP Address

As the router plays a role to manage and further protect its LAN, it interconnects groups of host PCs. Each of them has a private IP address assigned by the built-in DHCP server of the Vigor router. The router itself will also use the default **private IP** address: 192.168.1.1 to communicate with the local hosts. Meanwhile, Vigor router will communicate with other network devices through a **public IP** address. When the data flow passing through, the Network Address Translation (NAT) function of the router will dedicate to translate public/private addresses, and the packets will be delivered to the correct host PC in the local area network. Thus, all the host PCs can share a common Internet connection.

Get Your Public IP Address from ISP

In ADSL deployment, the PPP (Point to Point)-style authentication and authorization is required for bridging customer premises equipment (CPE). Point to Point Protocol over Ethernet (PPPoE) connects a network of hosts via an access device to a remote access concentrator or aggregation concentrator. This implementation provides users with significant ease of use. Meanwhile it provides access control, billing, and type of service according to user requirement.

When a router begins to connect to your ISP, a serial of discovery process will occur to ask for a connection. Then a session will be created. Your user ID and password is authenticated via **PAP** or **CHAP** with **RADIUS** authentication system. And your IP address, DNS server, and other related information will usually be assigned by your ISP.

Below shows the menu items for Internet Access.



4.1.2 PPPoE

To choose PPPoE as the accessing protocol of the internet, please select **PPPoE** from the **Internet Access** menu. The following web page will be shown.

PPPoE Client Mod	e		
PPPoE Setup		PPP/MP Setup	
PPPoE Link	🔘 Enable 💿 Disable	PPP Authentication	PAP or CHAP
ISP Access Setup)	🗹 Always On	
ISP Name		Idle Timeout	-1 second(s)
Username		IP Address Assignm (IPCP) WAN IP Alia	
Password		Fixed IP	O Yes No (Dynamic IP)
Index(1-15) in <u>Sc</u> =>,	hedule Setup:	Fixed IP Address	
WAN Connection	Detection	Oefault MAC Ad	dress
Mode	ARP Detect 🗸	Specify a MAC	Address
Ping IP		MAC Address:	
TTL:		00 .50 .7F 9A	.32 .71
WAN Backup Set	· · · · · · · · · · · · · · · · · · ·		
3G USB Moder			
Dial Backu	p Mode Disable 🚩		
Go to <u>3G l</u>	JSB Modem Setup		

OK

Enable/Disable	Click Enable for activating this function. If you click Disable , this function will be closed and all the settings that you adjusted in this page will be invalid.
ISP Access Setup	Enter your allocated username, password and authentication parameters according to the information provided by your ISP. Username – Type in the username provided by ISP in this field. Password – Type in the password provided by ISP in this field. Index (1-15) in Schedule Setup - You can type in four sets of time schedule for your request. All the schedules can be set previously in Application – Schedule web page and you can use the number that you have set in that web page.
WAN Connection Detection	 Such function allows you to verify whether network connection is alive or not through ARP Detect or Ping Detect. Mode – Choose ARP Detect or Ping Detect for the system to execute for WAN detection. Ping IP – If you choose Ping Detect as detection mode, you have to type IP address in this field for pinging. TTL (Time to Live) – Displays value for your reference. TTL value is set by telnet command.
WAN Backup Setup	3G USB Modem – If you install a 3G USB modem on the router, please Enable the Dial Backup Mode to perform file backup via USB device. After choosing Enable, please click the 3G USB



Modem link to access into the following page for configuring detailed settings.

WAN >> Internet Access

3G USB Modem Setup		
PPP Client Mode	◯ Enable	
SIM PIN code		
Modem Initial String	AT&FE0V1X1&D2&C1S0=0	(Default:AT&FE0V1X1&D2&C1S0=0)
APN Name		Apply
Modem Dial String	ATDT*99#	(Default:ATDT*99#)
PPP Username		(Optional)
PPP Password		(Optional)
Index(1-15) in Sched	<u>ule</u> Setup:	
=>,	,,	
	OK Cancel	Default

PPP Client Mode - Click Enable to activate this mode for WAN2.

SIM PIN code - Type PIN code of the SIM card that will be used to access Internet.

Modem Initial String - Such value is used to initialize USB modem. Please use the default value. If you have any question, please contact to your ISP.

APN Name – APN (Access Point Name) is provided by your ISP for identifying different access points. Simply click **Apply** to apply such name. Finally, you have to click **OK** to save the setting. **Apply** – Activate the function of identification.

Modem Dial String - Such value is used to dial through USB mode. Please use the default value. If you have any question, please contact to your ISP.

PPP Username - Type the PPP username (optional).

PPP Password - Type the PPP password (optional).

PPP/MP SetupPPP Authentication – Select **PAP only** or **PAP or CHAP** for PPP.If you want to connect to Internet all the time, you can check
Always On.

Idle Timeout – Set the timeout for breaking down the Internet after passing through the time without any action.

IP AddressUsually ISP dynamically assigns IP address to you each time youAssignment Methodconnect to it and request. In some case, your ISP provides service(IPCP)to always assign you the same IP address whenever you request.In this case, you can fill in this IP address in the Fixed IP field.Please contact your ISP before you want to use this function.

WAN IP Alias - If you have multiple public IP addresses and would like to utilize them on the WAN interface, please use WAN IP Alias. You can set up to 8 public IP addresses other than the current one you are using. Notice that this setting is available for WAN1 only.

🚰 http://19	92.168.1.5	- WAN IP Alias - Microsoft Inter	net Explorer 🛛 🔲 🗙
WAN IF	P Alias (Multi-NAT)	
Index	Enable	Aux. WAN IP	Join NAT IP Pool
1.	v	172.16.3.229	v
2.			
з.			
4.			
5.			
6.			
7.			
8.			
OK Clear All Close			

Fixed IP – Click **Yes** to use this function and type in a fixed IP address in the box of **Fixed IP Address**.

Default MAC Address – You can use **Default MAC Address** or specify another MAC address by typing on the boxes of MAC Address for the router.

Specify a MAC Address – Type the MAC address for the router manually.

After finishing all the settings here, please click **OK** to activate them.

4.1.3 Static or Dynamic IP

For static IP mode, you usually receive a fixed public IP address or a public subnet, namely multiple public IP addresses from your DSL or Cable ISP service providers. In most cases, a Cable service provider will offer a fixed public IP, while a DSL service provider will offer a public subnet. If you have a public subnet, you could assign an IP address or many IP address to the WAN interface.

To use **Static or Dynamic IP** as the accessing protocol of the internet, please choose **Static or Dynamic IP** mode from **Internet Access** menu. The following web page will be shown.



Internet Access >> Static or Dynamic IP

Static or Dynamic IP (DHCP Client)

Access Control		WAN IP Networ	k Settings	WAN IP Alias	
Broadband Access	💿 Enable 🔘 Disable	Obtain an IP			
Keep WAN Connection Enable PING to keep alive PING to the IP 0.0.0.0 PING Interval 0 minute(s) WAN physical type Auto negotiation WAN Connection Detection Mode ARP Detect		Router Name * Domain Name * Common Name * * : Required for some ISPs * Specify an IP address 192.168.5.29 Subnet Mask 255.255.255.0 Gateway IP Address 192.168.5.1 Image: Common Default MAC Address Specify a MAC Address MAC Address: MAC Address:			
Ping IP TTL:		00 .50 .7F	9A .32	. 71	
RIP Protocol Enable RIP		DNS Server IP Primary IP Add Secondary IP	lress		
WAN Backup Setup 3G USB Modem Dial Backup Mo Go to <u>3G USB I</u>					
	Г	OK			

Access Control	Click Enable for activating this function. If you click Disable , this function will be closed and all the settings that you adjusted in this page will be invalid.
Keep WAN Connection	Normally, this function is designed for Dynamic IP environments because some ISPs will drop connections if there is no traffic within certain periods of time. Check Enable PING to keep alive box to activate this function. PING to the IP - If you enable the PING function, please specify the IP address for the system to PING it for keeping alive. PING Interval - Enter the interval for the system to execute the PING operation.
WAN Physical Type	Choose Auto negotiation as the physical type for your router.
WAN Connection Detection	 Such function allows you to verify whether network connection is alive or not through ARP Detect or Ping Detect. Mode – Choose ARP Detect or Ping Detect for the system to execute for WAN detection. Ping IP – If you choose Ping Detect as detection mode, you have to type IP address in this field for pinging. TTL (Time to Live) – Displays value for your reference. TTL value is set by telnet command.
RIP Protocol	Routing Information Protocol is abbreviated as RIP (RFC1058) specifying how routers exchange routing tables information. Click Enable RIP for activating this function.



WAN Backup Setup
 3G USB Modem – If you install a 3G USB modem on the router, please Enable the Dial Backup Mode to perform file backup via USB device. After choosing Enable, please click the 3G USB Modem link to access into the following page for configuring detailed settings.

WAN >> Internet Access

3G USB Modem Setup	
PPP Client Mode	○ Enable ④ Disable
SIM PIN code	
Modem Initial String	AT&FE0V1X1&D2&C1S0=0 (Default:AT&FE0V1X1&D2&C1S0=0)
APN Name	Apply
Modem Dial String	ATDT*99# (Default:ATDT*99#)
PPP Username	(Optional)
PPP Password	(Optional)
Index(1-15) in <u>Scheo</u>	<u>lule</u> Setup:
->/	
	OK Cancel Default

PPP Client Mode - Click Enable to activate this mode for WAN2.

SIM PIN code - Type PIN code of the SIM card that will be used to access Internet.

Modem Initial String - Such value is used to initialize USB modem. Please use the default value. If you have any question, please contact to your ISP.

APN Name - APN(Access Point Name) is provided by your ISP for identifying different access points. Simply click **Apply** to apply such name. Finally, you have to click **OK** to save the setting. **Apply** – Activate the function of identification.

Modem Dial String - Such value is used to dial through USB mode. Please use the default value. If you have any question, please contact to your ISP.

PPP Username - Type the PPP username (optional).

PPP Password - Type the PPP password (optional).

WAN IP Network Settings This group allows you to obtain an IP address automatically and allows you type in IP address manually.

WAN IP Alias - If you have multiple public IP addresses and would like to utilize them on the WAN interface, please use WAN IP Alias. You can set up to 8 public IP addresses other than the current one you are using.



ø	🖄 http://192.168.1.5 - WAN IP Alias - Microsoft Internet Explorer 💦 🔲 🔀							
	WAN IP Alias (Multi-NAT)							
		Enable	Aux. WAN IP	Join NAT IP Pool				
			172.16.3.229					
	1.	v	172.10.3.229	V				
	2.							
	з.							
	4.							
	5.							
	6.							
	7.							
	8.							
	OK Clear All Close							

Obtain an IP address automatically – Click this button to obtain the IP address automatically if you want to use **Dynamic IP** mode. *Router Name:* Type in the router name provided by ISP. *Domain Name:* Type in the domain name that you have assigned.

Specify an IP address – Click this radio button to specify some data if you want to use **Static IP** mode.

IP Address: Type the IP address.

Subnet Mask: Type the subnet mask.

Gateway IP Address: Type the gateway IP address.

Default MAC Address : Click this radio button to use default MAC address for the router.

Specify a MAC Address: Some Cable service providers specify a specific MAC address for access authentication. In such cases you need to click the **Specify a MAC Address** and enter the MAC address in the MAC Address field.

DNS Server IP
AddressType in the primary IP address for the router if you want to use
Static IP mode. If necessary, type in secondary IP address for
necessity in the future.

4.1.4 PPTP/L2TP

To use **PPTP/L2TP** as the accessing protocol of the internet, please choose **PPTP/L2TP** from **Internet Access** menu. The following web page will be shown.

PPTP Client Mode			
PPTP Setup PPTP Link C Enable O Disable PPTP Server O	PPP Setup PPP Authentication PAP or CHAP ✓ ✓ Always On Idle Timeout -1		
ISP Access Setup Username Password	IP Address Assignment Method (IPCP) Fixed IP Yes Yes No (Dynamic IP) 		
Index(1-15) in <u>Schedule</u> Setup: =>,,,,,	 WAN IP Network Settings Obtain an IP address automatically Specify an IP address 		
WAN Backup Setup 3G USB Modem Dial Backup Mode Disable V Go to 3G USB Modem Backup Setup	IP Address 192.168.5.29 Subnet Mask 255.255.255.0		

PPTP Setup	 Enable - Click this radio button to enable a PPTP client to establish a tunnel to a DSL modem on the WAN interface. Disable - Click this radio button to close the connection through PPTP. PPTP Server - Specify the IP address of the PPTP/L2TP server if you enable PPTP/L2TP client mode.
ISP Access Setup	Username -Type in the username provided by ISP in this field. Password -Type in the password provided by ISP in this field. Index (1-15) in Schedule Setup - You can type in four sets of time schedule for your request. All the schedules can be set previously in Application – Schedule web page and you can use the number that you have set in that web page.
WAN Backup Setup	3G USB Modem – If you install a 3G USB modem on the router, please Enable the Dial Backup Mode to perform file backup via USB device. After choosing Enable, please click the 3G USB Modem link to access into the following page for configuring detailed settings.

OK



WAN >> Internet Access

3G USB Modem Setup

PPP Client Mode	◯ Enable	
SIM PIN code]
Modem Initial String	AT&FE0V1X1&D2&C1S0=0	(Default:AT&FE0V1X1&D2&C1S0=0)
APN Name		Apply
Modem Dial String	ATDT*99#	(Default:ATDT*99#)
PPP Username		(Optional)
PPP Password		(Optional)
Index(1-15) in <u>Sched</u>	ule Setup:	
=>,	,,	
	OK Cancel	Default

PPP Client Mode - Click Enable to activate this mode for WAN2.

SIM PIN code - Type PIN code of the SIM card that will be used to access Internet.

Modem Initial String - Such value is used to initialize USB modem. Please use the default value. If you have any question, please contact to your ISP.

APN Name - APN(Access Point Name) is provided by your ISP for identifying different access points. Simply click **Apply** to apply such name. Finally, you have to click **OK** to save the setting. **Apply** – Activate the function of identification.

Modem Dial String - Such value is used to dial through USB mode. Please use the default value. If you have any question, please contact to your ISP.

PPP Username - Type the PPP username (optional).

PPP Password - Type the PPP password (optional).

PPP Setup	PPP Authentication - Select PAP only or PAP or CHAP for PPP. Idle Timeout - Set the timeout for breaking down the Internet after passing through the time without any action.
IP Address Assignment Method(IPCP)	Fixed IP - Usually ISP dynamically assigns IP address to you each time you connect to it and request. In some case, your ISP provides service to always assign you the same IP address whenever you request. In this case, you can fill in this IP address in the Fixed IP field. Please contact your ISP before you want to use this function. Click Yes to use this function and type in a fixed IP address in the box.
	Fixed IP Address - Type a fixed IP address.
WAN IP Network Settings	Obtain an IP address automatically – Click this button to obtain the IP address automatically. Specify an IP address – Click this radio button to specify some

Dray Tek

data.

IP Address – Type the IP address. **Subnet Mask** – Type the subnet mask.

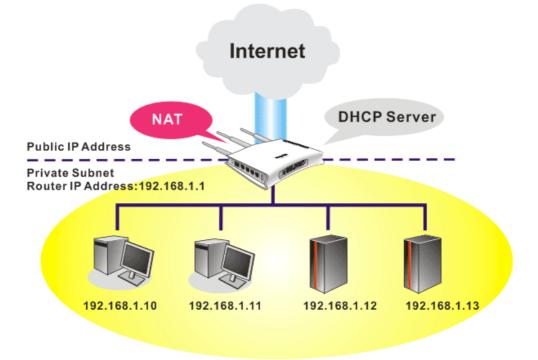
4.2 LAN

Local Area Network (LAN) is a group of subnets regulated and ruled by router. The design of network structure is related to what type of public IP addresses coming from your ISP.



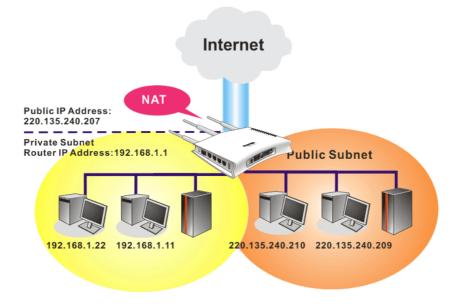
4.2.1 Basics of LAN

The most generic function of Vigor router is NAT. It creates a private subnet of your own. As mentioned previously, the router will talk to other public hosts on the Internet by using public IP address and talking to local hosts by using its private IP address. What NAT does is to translate the packets from public IP address to private IP address to forward the right packets to the right host and vice versa. Besides, Vigor router has a built-in DHCP server that assigns private IP address to each local host. See the following diagram for a briefly understanding.



In some special case, you may have a public IP subnet from your ISP such as 220.135.240.0/24. This means that you can set up a public subnet or call second subnet that each host is equipped with a public IP address. As a part of the public subnet, the Vigor router will serve for IP routing to help hosts in the public subnet to communicate with other public hosts or servers outside. Therefore, the router should be set as the gateway for public hosts.





What is Routing Information Protocol (RIP)

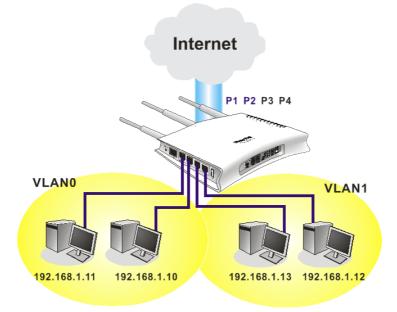
Vigor router will exchange routing information with neighboring routers using the RIP to accomplish IP routing. This allows users to change the information of the router such as IP address and the routers will automatically inform for each other.

What is Static Route

When you have several subnets in your LAN, sometimes a more effective and quicker way for connection is the **Static routes** function rather than other method. You may simply set rules to forward data from one specified subnet to another specified subnet without the presence of RIP.

What are Virtual LANs and Rate Control

You can group local hosts by physical ports and create up to 4 virtual LANs. To manage the communication between different groups, please set up rules in Virtual LAN (VLAN) function and the rate of each.



Dray Tek

4.2.2 General Setup

This page provides you the general settings for LAN.

Click LAN to open the LAN settings page and choose General Setup.

Ethernet TCP / IP and	I DHCP Setup				
LAN IP Network Confi	guration		DHCP Server Configura	tion	
For NAT Usage			💿 Enable Server 🔘 Disal	⊙Enable Server ○Disable Server	
1st IP Address	192.168.1.5		Relay Agent: 🔘 1st Subr	net 🔾 2nd Subnet	
1st Subnet Mask	255.255.255.0		Start IP Address	192.168.1.10	
For IP Routing Usage (🔵 Enable 💿 Disable		IP Pool Counts	50	
2nd IP Address	192.168.2.1		Gateway IP Address	192.168.1.5	
2nd Subnet Mask	255.255.255.0		DHCP Server IP Address		
	2nd Subnet DHCP Server		for Relay Agent		
			DNS Server IP Address		
RIP Protocol Control 🛛 Disable 🔽		Force DNS manual setting			
			Primary IP Address		
			Secondary IP Address		

1st IP Address	Type in private IP address for connecting to a local private network (Default: 192.168.1.1).
1st Subnet Mask	Type in an address code that determines the size of the network. (Default: 255.255.255.0/ 24)
For IP Routing Usage	Click Enable to invoke this function. The default setting is Disable .
2 nd IP Address	Type in secondary IP address for connecting to a subnet. (Default: 192.168.2.1/24)
2 nd Subnet Mask	An address code that determines the size of the network. (Default: 255.255.255.0/24)
2 nd DHCP Server	You can configure the router to serve as a DHCP server for the 2nd subnet.

Vigor2110 Series User's Guide

Dray Tek

Start IP Address IP Pool Counts		max. 10)	
Index Ma	tched MAC Addre	· · ·	en IP Address
MAC Address : Add	OK Clear /	Edit Clos	Cancel

Start IP Address: Enter a value of the IP address pool for the DHCP server to start with when issuing IP addresses. If the 2nd IP address of your router is 220.135.240.1, the starting IP address must be 220.135.240.2 or greater, but smaller than 220.135.240.254.

IP Pool Counts: Enter the number of IP addresses in the pool. The maximum is 10. For example, if you type 3 and the 2nd IP address of your router is 220.135.240.1, the range of IP address by the DHCP server will be from 220.135.240.2 to 220.135.240.11.

MAC Address: Enter the MAC Address of the host one by one and click **Add** to create a list of hosts to be assigned, deleted or edited IP address from above pool. Set a list of MAC Address for 2nd DHCP server will help router to assign the correct IP address of the correct subnet to the correct host. So those hosts in 2nd subnet won't get an IP address belonging to 1st subnet.

RIP Protocol Control Disable deactivates the RIP protocol. It will lead to a stoppage of the exchange of routing information between routers. (Default)

RIP Protocol Control

Disable	*
Disable	
1st Subnet	
2nd Subnet	

1st Subnet - Select the router to change the RIP information of the 1st subnet with neighboring routers.

2nd Subnet - Select the router to change the RIP information of the 2nd subnet with neighboring routers.

DHCP ServerDHCP stands for Dynamic Host Configuration Protocol. The
router by factory default acts a DHCP server for your network so
it automatically dispatch related IP settings to any local user
configured as a DHCP client. It is highly recommended that you
leave the router enabled as a DHCP server if you do not have a
DHCP server for your network.

If you want to use another DHCP server in the network other than the Vigor Router's, you can let Relay Agent help you to redirect the DHCP request to the specified location.

Enable Server - Let the router assign IP address to every host in the LAN.

Disable Server – Let you manually assign IP address to every host in the LAN.

Relay Agent – $(1^{st} subnet/2^{nd} subnet)$ Specify which subnet that DHCP server is located the relay agent should redirect the DHCP request to.

Start IP Address - Enter a value of the IP address pool for the DHCP server to start with when issuing IP addresses. If the 1st IP address of your router is 192.168.1.1, the starting IP address must be 192.168.1.2 or greater, but smaller than 192.168.1.254.

IP Pool Counts - Enter the maximum number of PCs that you want the DHCP server to assign IP addresses to. The default is 50 and the maximum is 253.

Gateway IP Address - Enter a value of the gateway IP address for the DHCP server. The value is usually as same as the 1st IP address of the router, which means the router is the default gateway.

DHCP Server IP Address for Relay Agent - Set the IP address of the DHCP server you are going to use so the Relay Agent can help to forward the DHCP request to the DHCP server.

DNS Server Configuration

DNS stands for Domain Name System. Every Internet host must have a unique IP address, also they may have a human-friendly, easy to remember name such as www.yahoo.com. The DNS server converts the user-friendly name into its equivalent IP address.

Force DNS manual setting - Force Vigor router to use DNS servers in this page instead of DNS servers given by the Internet Access server (PPPoE, PPTP, L2TP or DHCP server).

Primary IP Address -You must specify a DNS server IP address here because your ISP should provide you with usually more than one DNS Server. If your ISP does not provide it, the router will automatically apply default DNS Server IP address: 194.109.6.66 to this field.

Secondary IP Address - You can specify secondary DNS server IP address here because your ISP often provides you more than one DNS Server. If your ISP does not provide it, the router will automatically apply default secondary DNS Server IP address: 194.98.0.1 to this field.

The default DNS Server IP address can be found via Online Status:

System Status			System Uptime: 5:11:9
LAN Status	Primary I	DNS: 194.109.6.66	Secondary DNS: 168.95.1.1
IP Address	TX Packets	RX Packets	
192.168.1.5	9326	9487	

If both the Primary IP and Secondary IP Address fields are left empty, the router will assign its own IP address to local users as a DNS proxy server and maintain a DNS cache.

If the IP address of a domain name is already in the DNS cache, the router will resolve the domain name immediately. Otherwise, the router forwards the DNS query packet to the external DNS server by establishing a WAN (e.g. DSL/Cable) connection.



There are two common scenarios of LAN settings that stated in Chapter 4. For the configuration examples, please refer to that chapter to get more information for your necessity.

4.2.3 Static Route

Go to LAN to open setting page and choose Static Route.

LAN >>	Static	Route	Setup
	orario	1 Cource	occup

Static Route Configuration			Set to Factory Default View Routing Table		
Index	Destination Address	Status	Index	Destination Address	Status
<u>1.</u>	???	?	<u>6.</u>	???	?
<u>2.</u>	???	?	<u>7.</u>	???	?
<u>3.</u>	???	?	<u>8.</u>	???	?
<u>4.</u>	???	?	<u>9.</u>	???	?
<u>5.</u>	???	?	<u>10.</u>	???	?

Status: v --- Active, x --- Inactive, ? --- Empty

Index	The number (1 to 10) under Index allows you to open next page to set up static route.
Destination Address	Displays the destination address of the static route.
Status	Displays the status of the static route.
Viewing Routing Table	Displays the routing table for your reference. Diagnostics >> View Routing Table

Key: C - connected, S - static, R - RIP, * - default, ~ - private			
2~	192.168.1.0/	255.255.255.0 is directly connected, LAN	l

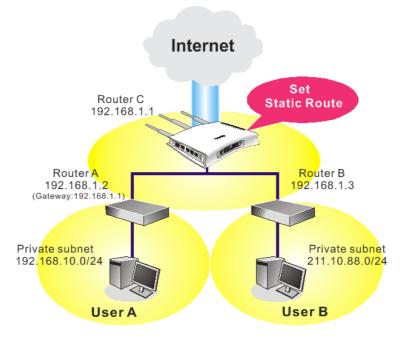
Add Static Routes to Private and Public Networks

Here is an example of setting Static Route in Main Router so that user A and B locating in different subnet can talk to each other via the router. Assuming the Internet access has been configured and the router works properly:

- use the Main Router to surf the Internet.
- create a private subnet 192.168.10.0 using an internal Router A (192.168.1.2)
- create a public subnet 211.100.88.0 via an internal Router B (192.168.1.3).
- have set Main Router 192.168.1.1 as the default gateway for the Router A 192.168.1.2.

Before setting Static Route, user A cannot talk to user B for Router A can only forward recognized packets to its default gateway Main Router.





1. Go to LAN page and click General Setup, select 1st Subnet as the RIP Protocol Control. Then click the OK button.

Note: There are two reasons that we have to apply RIP Protocol Control on 1st Subnet. The first is that the LAN interface can exchange RIP packets with the neighboring routers via the 1st subnet (192.168.1.0/24). The second is that those hosts on the internal private subnets (ex. 192.168.10.0/24) can access the Internet via the router, and continuously exchange of IP routing information with different subnets.

2. Click the LAN - Static Route and click on the Index Number 1. Check the Enable box. Please add a static route as shown below, which regulates all packets destined to 192.168.10.0 will be forwarded to 192.168.1.2. Click OK.

🗹 Enable		
	Destination IP Address	192.168.10.0
	Subnet Mask	255.255.255.0
	Gateway IP Address	192.168.1.2
	Network Interface	LAN 🔽

3. Return to **Static Route Setup** page. Click on another **Index Number** to add another static route as show below, which regulates all packets destined to 211.100.88.0 will be forwarded to 192.168.1.3.

LAN >> Static Route Setup



LAN >> Static Route Setup

🗹 Enable		
	Destination IP Address	211.100.88.0
	Subnet Mask	255.255.255.0
	Gateway IP Address	192.168.1.3
	Network Interface	LAN 🔽

4. Go to **Diagnostics** and choose **Routing Table** to verify current routing table.

Diagnostics >> View Routing Table

Key: C	- connected, S -	static, R - RIP, * - default, ~ - priva	te	^
3~	192.168.10.0/	255.255.255.0 via 192.168.1.2, LAN		
- ~	192.168.1.0/	255.255.255.0 is directly connected,	LAN	
5~	211.100.88.0/	255.255.255.0 via 192.168.1.3, LAN		
				- 14

4.2.4 VLAN

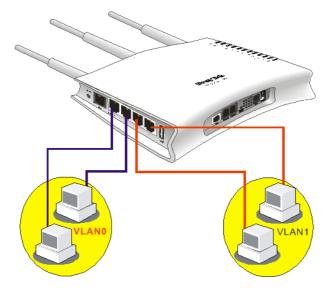
Virtual LAN function provides you a very convenient way to manage hosts by grouping them based on the physical port. You can also manage the in/out rate of each port. Go to LAN page and select VLAN. The following page will appear. Click **Enable** to invoke VLAN function.

Z Enable				
	P1	P2	P3	P4
VLANO				
VLAN1				
VLAN2				
VLAN3				

LAN >> VLAN Configuration

To add or remove a VLAN, please refer to the following example.

1. If, VLAN 0 is consisted of hosts linked to P1 and P2 and VLAN 1 is consisted of hosts linked to P3 and P4.



LAN >> VLAN Configuration

2. After checking the box to enable VLAN function, you will check the table according to the needs as shown below.

🗹 Enable					
		P1	P2	P3	P4
	VLANO	v	v		
	VLAN1			v	
	VLAN2				
	VLAN3				

To remove VLAN, uncheck the needed box and click **OK** to save the results.



4.2.5 Bind IP to MAC

This function is used to bind the IP and MAC address in LAN to have a strengthening control in network. When this function is enabled, all the assigned IP and MAC address binding together cannot be changed. If you modified the binding IP or MAC address, it might cause you not access into the Internet.

Click LAN and click Bind IP to MAC to open the setup page.

LAN >>	Bind	IP to	MAC	
--------	------	-------	-----	--

Bind IP to MAC		
Note: IP-MAC binding presets DHCP Allocati	ons.	
If you select Strict Bind, unspecified	LAN clients cannot access f	the Internet.
● Enable ○ Disable ○ Strict Bind ■		
ARP Table Select All Sort Refresh	IP Bind List	Select All Sort
IP Address Mac Address 192.168.1.1 00-50-7F-DD-15-18 192.168.1.10 00-0E-A6-2A-D5-A1	Index IP Address	Mac Address
Add and Edit IP Address		
Add	Edit Delete	

OK

Enable	Click this radio button to invoke this function. However, IP/MAC which is not listed in IP Bind List also can connect to Internet.
Disable	Click this radio button to disable this function. All the settings on this page will be invalid.
Strict Bind	Click this radio button to block the connection of the IP/MAC which is not listed in IP Bind List.
ARP Table	This table is the LAN ARP table of this router. The information for IP and MAC will be displayed in this field. Each pair of IP and MAC address listed in ARP table can be selected and added to IP Bind List by clicking Add below.
Add and Edit	 IP Address - Type the IP address that will be used for the specified MAC address. Mac Address - Type the MAC address that is used to bind with the assigned IP address.
Refresh	It is used to refresh the ARP table. When there is one new PC added to the LAN, you can click this link to obtain the newly ARP table information.
IP Bind List	It displays a list for the IP bind to MAC information.



Add	It allows you to add the one you choose from the ARP table or the IP/MAC address typed in Add and Edit to the table of IP Bind List.
Edit	It allows you to edit and modify the selected IP address and MAC address that you create before.
Remove	You can remove any item listed in IP Bind List . Simply click and select the one, and click Remove . The selected item will be removed from the IP Bind List .

Note: Before you select **Strict Bind**, you have to bind one set of IP/MAC address for one PC. If not, no one of the PCs can access into Internet. And the web configurator of the router might not be accessed.

4.3 NAT

Usually, the router serves as an NAT (Network Address Translation) router. NAT is a mechanism that one or more private IP addresses can be mapped into a single public one. Public IP address is usually assigned by your ISP, for which you may get charged. Private IP addresses are recognized only among internal hosts.

When the outgoing packets destined to some public server on the Internet reach the NAT router, the router will change its source address into the public IP address of the router, select the available public port, and then forward it. At the same time, the router shall list an entry in a table to memorize this address/port-mapping relationship. When the public server response, the incoming traffic, of course, is destined to the router's public IP address and the router will do the inversion based on its table. Therefore, the internal host can communicate with external host smoothly.

The benefit of the NAT includes:

- Save cost on applying public IP address and apply efficient usage of IP address. NAT allows the internal IP addresses of local hosts to be translated into one public IP address, thus you can have only one IP address on behalf of the entire internal hosts.
- Enhance security of the internal network by obscuring the IP address. There are many attacks aiming victims based on the IP address. Since the attacker cannot be aware of any private IP addresses, the NAT function can protect the internal network.

On NAT page, you will see the private IP address defined in RFC-1918. Usually we use the 192.168.1.0/24 subnet for the router. As stated before, the NAT facility can map one or more IP addresses and/or service ports into different specified services. In other words, the NAT function can be achieved by using port mapping methods.

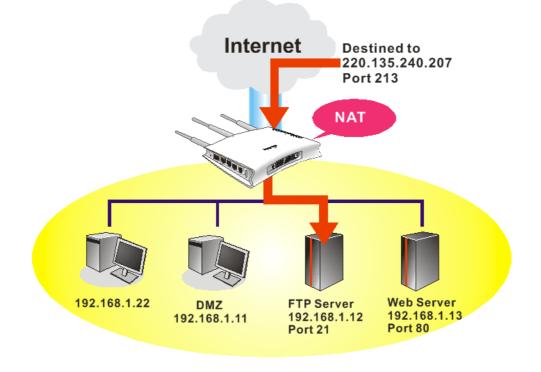
Below shows the menu items for NAT.

```
NAT
Port Redirection
DMZ Host
Open Ports
```

4.3.1 Port Redirection

Port Redirection is usually set up for server related service inside the local network (LAN), such as web servers, FTP servers, E-mail servers etc. Most of the case, you need a public IP address for each server and this public IP address/domain name are recognized by all users. Since the server is actually located inside the LAN, the network well protected by NAT of the router, and identified by its private IP address/port, the goal of Port Redirection function is to





forward all access request with public IP address from external users to the mapping private IP address/port of the server.

The port redirection can only apply to incoming traffic.

NAT >> Port Redirection

To use this function, please go to **NAT** page and choose **Port Redirection** web page. The **Port Redirection Table** provides 20 port-mapping entries for the internal hosts.

ion		Set to F	actory Default
Service Name	Public Port	Private IP	Status
			X
			x
			×
			x
			×
			x
			×
			x
			x
			×
	Service Name	Service Name Public Port	Service Name Public Port Private IP Image: Service Name Image: Service Name Image: Service Name Image: Service Name Image: Service Name Image: Service Name Image: Service Name Image: Service Name Image: Service Name Image: Service Name Image: Service Name Image: Service Name Image: Service Name Image: Service Name Image: Service Name Image: Service Name Image: Service Name Image: Service Name Image: Service Name Image: Service Name Image: Service Name Image: Service Name Image: Service Name Image: Service Name Image: Service Name Image: Service Name Image: Service Name Image: Service Name Image: Service Name Image: Service Name Image: Service Name Image: Service Name Image: Service Name Image: Service Name Image: Service Name Image: Service Name Image: Service Name Image: Service Name Image: Service Name Image: Service Name Image: Service Name Image: Service Name Image: Service Name Image: Service Name Image: Service Name Image: Service Name Image: Service Name<

Press any number under Index to access into next page for configuring port redirection.



NAT >> Port Redirection

Index No. 1	
🗖 Enable	
Mode	Single 💌
Service Name	Single Range
Protocol	💙
WAN IP	1.All
Public Port	0
Private IP	
Private Port	0

Note: In "Range" Mode the End IP will be calculated automatically once the Public Port and Start IP have been entered.

	OK Clear Cancel
Enable	Check this box to enable such port redirection setting.
Mode	Two options (Single and Range) are provided here for you to choose. To set a range for the specific service, select Range . In Range mode, if the public port (start port and end port) and the starting IP of private IP had been entered, the system will calculate and display the ending IP of private IP automatically.
Service Name	Enter the description of the specific network service.
Protocol	Select the transport layer protocol (TCP or UDP).
WAN IP	Select the WAN IP used for port redirection. There are eight WAN IP alias that can be selected and used for port redirection. The default setting is All which means all the incoming data from any port will be redirected to specified range of IP address and port.
Public Port	Specify which port can be redirected to the specified Private IP and Port of the internal host. If you choose Range as the port redirection mode, you will see two boxes on this field. Simply type the required number on the first box. The second one will be assigned automatically later.
Private IP	Specify the private IP address of the internal host providing the service. If you choose Range as the port redirection mode, you will see two boxes on this field. Type a complete IP address in the first box (as the starting point) and the fourth digits in the second box (as the end point).
Private Port	Specify the private port number of the service offered by the internal host.

Note that the router has its own built-in services (servers) such as Telnet, HTTP and FTP etc. Since the common port numbers of these services (servers) are all the same, you may need to reset the router in order to avoid confliction.

For example, the built-in web configurator in the router is with default port 80, which may conflict with the web server in the local network, http://192.168.1.13:80. Therefore, you need to **change the router's http port to any one other than the default port 80** to avoid conflict, such as 8080. This can be set in the **System Maintenance** >>**Management Setup**. You then will access the admin screen of by suffixing the IP address with 8080, e.g., http://192.168.1.1:8080 instead of port 80.

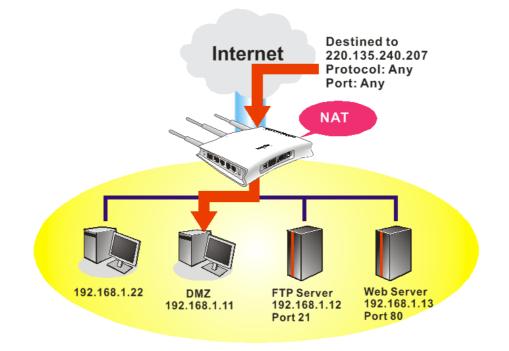


System Maintenance >> Management

Management 9	Setup			
Management	Access Co	ontrol	Management Port Setu	р
Allow mana	gement fro	m the Internet	💿 User Define Ports (Default Ports
FTP Ser	ver		Telnet Port	23 (Default: 23)
HTTP Se	erver		HTTP Port	80 (Default: 80)
HTTPS S	Server		HTTPS Port	443 (Default: 443)
🗹 Telnet S	Server			
SSH Ser	ver		FTP Port	21 (Default: 21)
🗹 Disable PIN	G from the	Internet	SSH Port	22 (Default: 22)
			CNMD Cotur	
Access List	_		SNMP Setup	
List I	P	Subnet Mask	Enable SNMP Agent	
1		*	Get Community	public
2		*	Set Community	private
3		~	Manager Host IP	
			Trap Community	public
			Notification Host IP	
			Trap Timeout	10 seconds
		0	K	

4.3.2 DMZ Host

As mentioned above, **Port Redirection** can redirect incoming TCP/UDP or other traffic on particular ports to the specific private IP address/port of host in the LAN. However, other IP protocols, for example Protocols 50 (ESP) and 51 (AH), do not travel on a fixed port. Vigor router provides a facility **DMZ Host** that maps ALL unsolicited data on any protocol to a single host in the LAN. Regular web surfing and other such Internet activities from other clients will continue to work without inappropriate interruption. **DMZ Host** allows a defined internal user to be totally exposed to the Internet, which usually helps some special applications such as Netmeeting or Internet Games etc.



The security properties of NAT are somewhat bypassed if you set up DMZ host. We suggest you to add additional filter rules or a secondary firewall.

Click **DMZ Host** to open the following page:

ΝΔΤ		Host	Setu	h
INAI	//	nosi	Setu	J

N 1	
None 💌	
Private IP	Choose PC
MAC Address of the True IP DMZ Host	00 . 00 . 00 .00 . 00 . 00
Note: When a True-IP DMZ host is turne be always on.	d on, it will force the router's WAN connection to

If you previously have set up **WAN Alias** for **PPPoE** or **Static or Dynamic IP** mode, you will find them in **Aux. WAN IP** for your selection.

1	NAT >> D	MZ Host S	etup		
ļ	OMZ Host	Setup			
	WAN 1 Index	Enable	Aux. WAN IP	Private IP	
	1.		172.16.3.229		Choose PC
	2.		162.168.1.55		Choose PC
				OK Clear	
E	nable		Check to en	able the DMZ Host fun	ction.
P	rivate II	Р	Enter the pr select one.	ivate IP address of the I	DMZ host, or click Choose PC t

Vigor2110 Series User's Guide



Choose PC

Click this button and then a window will automatically pop up, as depicted below. The window consists of a list of private IP addresses of all hosts in your LAN network. Select one private IP address in the list to be the DMZ host.



When you have selected one private IP from the above dialog, the IP address will be shown on the following screen. Click **OK** to save the setting.

NAT >> DMZ Host Setup

WAN 1 Index	Enable	Aux. WAN IP	Private IP	
1.	V	172.16.3.229	192.168.1.10	Choose PC
2.		162.168.1.55		Choose PC

4.3.3 Open Ports

Open Ports allows you to open a range of ports for the traffic of special applications.

Common application of Open Ports includes P2P application (e.g., BT, KaZaA, Gnutella, WinMX, eMule and others), Internet Camera etc. Ensure that you keep the application involved up-to-date to avoid falling victim to any security exploits.

Click **Open Ports** to open the following page:

NAT >> Open Ports

Status	Local IP Address	Aux. WAN IP	Comment	Index
×				<u>1.</u>
х				<u>2.</u>
х				<u>3.</u>
×				<u>4.</u>
х				<u>5.</u>
×				<u>6.</u>
х				<u>7.</u>
×				<u>8.</u>
х				<u>9.</u>
X				<u>10.</u>



Index	Indicate the relative number for the particular entry that you want to offer service in a local host. You should click the appropriate index number to edit or clear the corresponding entry.
Comment	Specify the name for the defined network service.
Local IP Address	Display the private IP address of the local host offering the service.
Status	Display the state for the corresponding entry. X or V is to represent the Inactive or Active state.

To add or edit port settings, click one index number on the page. The index entry setup page will pop up. In each index entry, you can specify **10** port ranges for diverse services.

NAT >> Open Ports >> Edit Open Ports

✓ E	inable Op	en Ports	:					
		Comm	ent	P2P				
		WAN I	Р	172.	16.3.229	~		
		Local	Computer	192.1	168.1.10	Choose	e PC	
	Proto	col	Start Port	End Port		Protocol	Start Port	End Port
1.	TCP	*	4500	4700	6.	💙	0	0
2.	UDP	*	4500	4700	7.	🖌	0	0
3.		*	0	0	8.	💙	0	0
		~	0	0	9.	💙	0	0
5.		~	0	0	10.	💙	0	0

Enable Open Ports	Check to enable this entry.
Comment	Make a name for the defined network application/service.
WAN IP	Specify the WAN IP address that will be used for this entry. This setting is available when WAN IP Alias is configured.
Local Computer	Enter the private IP address of the local host or click Choose PC to select one.
Choose PC	Click this button and, subsequently, a window having a list of private IP addresses of local hosts will automatically pop up. Select the appropriate IP address of the local host in the list.
Protocol	Specify the transport layer protocol. It could be TCP , UDP , or (none) for selection.
Start Port	Specify the starting port number of the service offered by the local host.
End Port	Specify the ending port number of the service offered by the local host.



4.4 Hardware Acceleration

Hardware-base Acceleration Engine, also named Protocol Processing Engine API is the function that Draytek provides to extremely speed up the NAT performance.

While the hardware acceleration mechanism is activated, most of the bandwidth usage will be concentrated on the specific sessions which increase transmission speed to get ultimately accelerated.

Hardwar	e Accelera	ation >> S	etup					
Mode:	Disabled 1	*						
Protocol:	TCP UDP Accelerate most heavy traffic sessions							
Option:								
	Apply the <u>Class Rule</u> in Quality of Service							
	O Specif	ic Hosts:						
	Index	Enable	Start port	End port	Private IP			
	1.		0	0		Choose		
	2.		0	0		Choose		
	з.		0	0		Choose		
	4.		0	0		Choose		
	5.		0	0		Choose		
Mode		sett Au The ses Ma spe	ing. to – Choose the e router can de sion to earn the mual – Choose cify which pro- cify which pro- code: Mar Disa	his option to e etect heavy tra the bandwidth j this option to tocool will be tual v bled	leration mechanism. execute this function affic session and acc per requested. to set rules manually applied. Then, choo	automatically. elerate that 7. You have to		
Protocol Option		TC	P and UDP.	, there are two	o protocols provided ee options offered fo			
ohnon		111 1	inducian inouc	, more are thi	ee options offered it	J you to appiy.		

Accelerate most heavy traffic sessions – This function is the same as in Auto mode.
 Apply the Class Rule in Quality of Service – Rules configured in

QoS will be applied. **Specific Hosts** – You can set five hosts in this page to apply hardware acceleration. Please check Enable box, type Start port and End port, and specify Private IP for each host respectively.

When you configure all of the settings, click **OK** to save the configuration.

Note: Bandwidth allocation to other non-specified session would be affected as the acceleration engine is activated.



4.5 Firewall

4.5.1 Basics for Firewall

While the broadband users demand more bandwidth for multimedia, interactive applications, or distance learning, security has been always the most concerned. The firewall of the Vigor router helps to protect your local network against attack from unauthorized outsiders. It also restricts users in the local network from accessing the Internet. Furthermore, it can filter out specific packets that trigger the router to build an unwanted outgoing connection.

Firewall Facilities

The users on the LAN are provided with secured protection by the following firewall facilities:

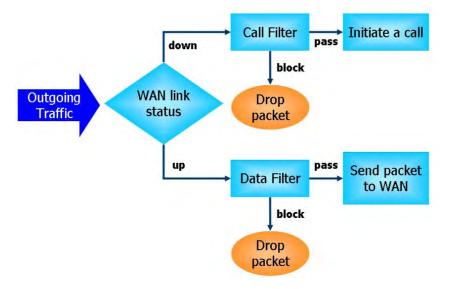
- User-configurable IP filter (Call Filter/ Data Filter).
- Stateful Packet Inspection (SPI): tracks packets and denies unsolicited incoming data
- Selectable Denial of Service (DoS) /Distributed DoS (DDoS) attacks protection

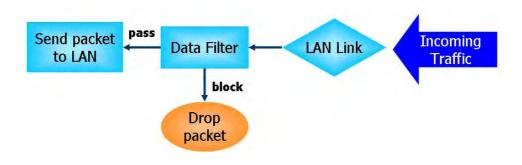
IP Filters

Depending on whether there is an existing Internet connection, or in other words "the WAN link status is up or down", the IP filter architecture categorizes traffic into two: **Call Filter** and **Data Filter**.

- **Call Filter** When there is no existing Internet connection, **Call Filter** is applied to all traffic, all of which should be outgoing. It will check packets according to the filter rules. If legal, the packet will pass. Then the router shall **"initiate a call"** to build the Internet connection and send the packet to Internet.
- **Data Filter** When there is an existing Internet connection, **Data Filter** is applied to incoming and outgoing traffic. It will check packets according to the filter rules. If legal, the packet will pass the router.

The following illustrations are flow charts explaining how router will treat incoming traffic and outgoing traffic respectively.





Stateful Packet Inspection (SPI)

Stateful inspection is a firewall architecture that works at the network layer. Unlike legacy static packet filtering, which examines a packet based on the information in its header, stateful inspection builds up a state machine to track each connection traversing all interfaces of the firewall and makes sure they are valid. The stateful firewall of Vigor router not just examine the header information also monitor the state of the connection.

Denial of Service (DoS) Defense

The **DoS Defense** functionality helps you to detect and mitigate the DoS attack. The attacks are usually categorized into two types, the flooding-type attacks and the vulnerability attacks. The flooding-type attacks will attempt to exhaust all your system's resource while the vulnerability attacks will try to paralyze the system by offending the vulnerabilities of the protocol or operation system.

The **DoS Defense** function enables the Vigor router to inspect every incoming packet based on the attack signature database. Any malicious packet that might duplicate itself to paralyze the host in the secure LAN will be strictly blocked and a Syslog message will be sent as warning, if you set up Syslog server.

Also the Vigor router monitors the traffic. Any abnormal traffic flow violating the pre-defined parameter, such as the number of thresholds, is identified as an attack and the Vigor router will activate its defense mechanism to mitigate in a real-time manner.

The below shows the attack types that DoS/DDoS defense function can detect:

- 1. SYN flood attack
- 2. UDP flood attack
- 3. ICMP flood attack
- 4. Port Scan attack
- 5. IP options
- 6. Land attack
- 7. Smurf attack
- 8. Trace route

- 9. SYN fragment
- 10. Fraggle attack
- 11. TCP flag scan
- 12. Tear drop attack
- 13. Ping of Death attack
- 14. ICMP fragment
- 15. Unknown protocol

Below shows the menu items for Firewall.

Firewall General S

- Filter Setup
- BoS Defense



4.5.2 General Setup

General Setup allows you to adjust settings of IP Filter and common options. Here you can enable or disable the **Call Filter** or **Data Filter**. Under some circumstance, your filter set can be linked to work in a serial manner. So here you assign the **Start Filter Set** only. Also you can configure the **Log Flag** settings, **Apply IP filter to VPN incoming packets**, and **Accept incoming fragmented UDP packets**.

Click Firewall and click General Setup to open the general setup page.

Firewall	>> (General	Setup
----------	------	---------	-------

Call Filter	💿 Enable	Start Filter S	Set Set#1 🔽
	🔘 Disable		
Data Filter	💿 Enable	Start Filter 9	Get Set#2 🔽
	🔘 Disable		
Actions for defa	ult rule:		
Application		Action/Profile	Syslog
Filter		Pass 💌	
IM/P2P Filter		None 💌	
URL Content Filte	1	None 💌	
Web Content Filte	<u>) (</u>	None 🛩	
Advance Setting		Edit	

	OK Cancel
Call Filter	Check Enable to activate the Call Filter function. Assign a start filter set for the Call Filter.
Data Filter	Check Enable to activate the Data Filter function. Assign a start filter set for the Data Filter.
Filter	Select Pass or Block for the packets that do not match with the filter rules. Pass Pass Block
IM/P2P Filter	Select a CSM profile for global IM/P2P application blocking. All the hosts in LAN must follow the standard configured in the CSM profile selected here. For detailed information, refer to the section of CSM profile setup. For troubleshooting needs, you can specify to record information for IM/P2P by checking the Log box. It will be sent to Syslog server. Please refer to section 4.14.4 Syslog/Mail Alert for more detailed information.
URL Content Filter	Select one of the URL Content Filter profile settings (created in CSM>> URL Content Filter) for applying with this router. Please set at least one profile for choosing in CSM>> URL Content Filter web page first. For troubleshooting needs, you can specify to record information for URL Content Filter by checking the Log box. It



	will be sent to Syslog server. Please refer to section 4.14.4 Syslog/Mail Alert for more detailed information.
Web Content Filter	Select one of the Web Content Filter profile settings (created in CSM>> Web Content Filter) for applying with this router. Please set at least one profile for anti-virus in CSM>> Web Content Filter web page first. For troubleshooting needs, you can specify to record information for Web Content Filter by checking the Log box. It will be sent to Syslog server. Please refer to section 4.14.4 Syslog/Mail Alert for more detailed information.
Syslog	For troubleshooting needs you can specify the filter log and/or CSM log here by checking the box. The log will be displayed on Draytek Syslog window.

Advance Setting Click Edit to open the following window. However, it is strongly recommended to use the default settings here.

//192.168.1.5/doc/ipfgenadv.htm	n - Microsoft Internet Explore:	
Firewall >> General Set	up	
- Advance Setting		
Codepage	ANSI(1252)-Latin I	~
Window size:	65535	
Session timeout:	1440	Minute
	OK Close	

Codepage - This function is used to compare the characters among different languages. Choose correct codepage can help the system obtaining correct ASCII after decoding data from URL and enhance the correctness of URL Content Filter. The default value for this setting is ANSI 1252 Latin I. If you do not choose any codepage, no decoding job of URL will be processed. Please use the drop-down list to choose a codepage.

If you do not have any idea of choosing suitable codepage, please open Syslog. From Codepage Information of Setup dialog, you will see the recommended codepage listed on the dialog box.

Controls	192.168.1.1 Vigor RX Packets 15285	WAN Information WAN1 IP (Fixed) 172.16.2.213 WAN2 IP (Fixed)
Setup Tool Setup Telnet Read-out Set Codepage To Select Windows Version: 5.01.260 RECOMMENDED CODEP 950 (ANSI/OEM - Traditic 00a1.21 00a6:7c 00a9:63 00	0 AGE: mal Chinese Big5)) 2:32 00b3:33 00b9:31 00ba:6f 0

Window size – It determines the size of TCP protocol (0~65535). The more the value is, the better the performance will be. However, if the network is not stable, small value will be proper.

Session timeout–Setting timeout for sessions can make the best utilization of network resources. However, Queue timeout is configured for TCP protocol only; session timeout is configured for the data flow which matched with the firewall rule.

Some on-line games (for example: Half Life) will use lots of fragmented UDP packets to transfer game data. Instinctively as a secure firewall, Vigor router will reject these fragmented packets to prevent attack unless you enable "Accept large incoming fragmented UDP or ICMP Packets". By checking this box, you can play these kinds of on-line games. If security concern is in higher priority, you cannot enable "Accept large incoming fragmented UDP or ICMP Packets".

4.5.3 Filter Setup

Click Firewall and click Filter Setup to open the setup page.

Firewal	>>	Filter	Setup
---------	----	--------	-------

Filter S	etup		Set to Factory Default
Set	Comments	Set	Comments
<u>1.</u>	Default Call Filter	<u>7.</u>	
<u>2.</u>	Default Data Filter	<u>8.</u>	
<u>3.</u>		<u>9.</u>	
<u>4.</u>		<u>10.</u>	
<u>5.</u>		<u>11.</u>	
<u>6.</u>		<u>12.</u>	

To edit or add a filter, click on the set number to edit the individual set. The following page will be shown. Each filter set contains up to 7 rules. Click on the rule number button to edit each rule. Check **Active** to enable the rule.

Firewall >>	Filter Setu	p >> Edit	Filter Set
-------------	-------------	-----------	------------

omments : D	efault Call Filter	 Comments		Move Up	Move Down
		Block NetBios		move op	Down
2		BIOCK NECDIO	,	<u>UP</u>	<u>Down</u>
3				<u>UP</u>	<u>Down</u>
4				<u>UP</u>	<u>Down</u>
5				<u>UP</u>	<u>Down</u>
6				<u>UP</u>	<u>Down</u>
7				<u>UP</u>	
				Next Filte	r Set None 📘

Filter Rule

Click a button numbered $(1 \sim 7)$ to edit the filter rule. Click the button will open Edit Filter Rule web page. For the detailed information, refer to the following page.



Active	Enable or disable the filter rule.
Comment	Enter filter set comments/description. Maximum length is 23–character long.
Move Up/Down	Use Up or Down link to move the order of the filter rules.
Next Filter Set	Set the link to the next filter set to be executed after the current filter run. Do not make a loop with many filter sets.

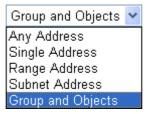
To edit Filter Rule, click the Filter Rule index button to enter the Filter Rule setup page.

Firewall >> Edit Filter Set >> Edit Filter Rule

Comments:	Block NetBios	
index(1-15) in <u>Schedule</u> Setup:		
Direction:	LAN -> WAN 🗸	
Source IP:	Any	Edit
Destination IP:	Any	Edit
Service Type:	TCP/UDP, Port: from 137~139 to undefined	Edit
Fragments:	Don't Care 💌	
Application	Action/Profile	Syslog
Filter:	Block Immediately 🔽	
Branch to Other Filter Set:	None 🗸	
IM/P2P Filter:	None 👻	
URL Content Filter	None 🗸	
Web Content Filter	None 😪	
Advance Setting	Edit	

Check to enable the Filter Rule	Check this box to enable the filter rule.
Comments	Enter filter set comments/description. Maximum length is 14- character long.
Index(1-15)	Set PCs on LAN to work at certain time interval only. You may choose up to 4 schedules out of the 15 schedules pre-defined in Applications >> Schedule setup. The default setting of this field is blank and the function will always work.
Direction	Set the direction of packet flow (LAN->WAN/WAN->LAN). It is for Data Filter only. For the Call Filter , this setting is not available since Call Filter is only applied to outgoing traffic.
Source/Destination IP	Click Edit to access into the following dialog to choose the source/destination IP or IP ranges.
	To set the IP address manually, please choose Any Address/Single Address/Range Address/Subnet Address as the Address Type and type them in this dialog. In addition, if you want to use the IP range from defined groups or objects, please choose Group and Objects

as the Address Type.



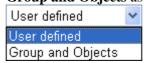
From the **IP Group** drop down list, choose the one that you want to apply. Or use the **IP Object** drop down list to choose the object that you want.

Service Type

Click **Edit** to access into the following dialog to choose a suitable service type.

Service Type	User defined
Protocol	
Source Port	= 🖌 137 ~ 139
Destination Port	= 🖌 1 ~ 65535
Service Group	None 💟
or <u>Service Object</u>	None 🔛
or Service Object	None 🔽
or Service Object	None 💙

To set the service type manually, please choose **User defined** as the Service Type and type them in this dialog. In addition, if you want to use the service type from defined groups or objects, please choose **Group and Objects** as the Service Type.



Protocol - Specify the protocol(s) which this filter rule will apply to. **Source/Destination Port -**

(=) – when the first and last value are the same, it indicates one port; when the first and last values are different, it indicates a range for the port and available for this service type.

(*!*=) – when the first and last value are the same, it indicates all the ports except the port defined here; when the first and last values are different, it indicates that all the ports except the range defined here are available for this service type.

(>) – the port number greater than this value is available.

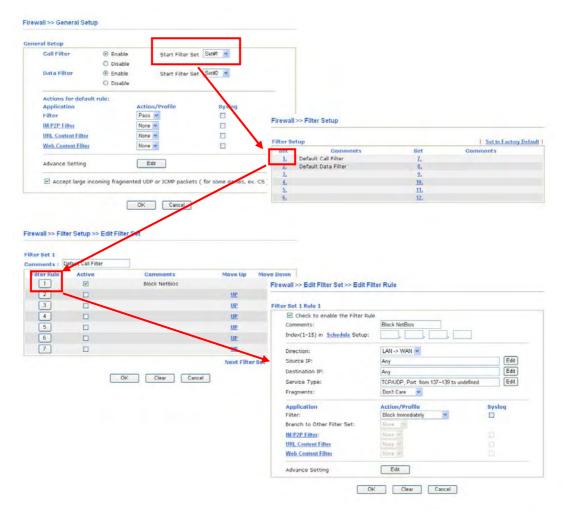
(<) – the port number less than this value is available for this profile.</p>
Service Group/Object - Use the drop down list to choose the one that you want.



Fragments	Specify the action for fragmented packets. And it is used for Data Filter only. <i>Don't care</i> -No action will be taken towards fragmented packets. <i>Unfragmented</i> -Apply the rule to unfragmented packets. <i>Fragmented</i> - Apply the rule to fragmented packets. <i>Too Short</i> - Apply the rule only to packets that are too short to contain a complete header.
Filter	 Specifies the action to be taken when packets match the rule. Block Immediately - Packets matching the rule will be dropped immediately. Pass Immediately - Packets matching the rule will be passed immediately. Block If No Further Match - A packet matching the rule, and that does not match further rules, will be dropped. Pass If No Further Match - A packet matching the rule, and that does not match further rules, will be passed through.
Branch to other Filter Set	If the packet matches the filter rule, the next filter rule will branch to the specified filter set. Select next filter rule to branch from the drop-down menu. Be aware that the router will apply the specified filter rule for ever and will not return to previous filter rule any more.
Content Security Management	All the packets/connections within the range configured in the above conditions must follow the standard configured in the CSM profile selected here. For detailed information, refer to the section of CSM profile setup.
SysLog	For troubleshooting needs you can specify the filter log and/or CSM log here. Check the corresponding box to enable the log function. Then, the filter log and/or CSM log will be shown on Draytek Syslog window.

Example

As stated before, all the traffic will be separated and arbitrated using on of two IP filters: call filter or data filter. You may preset 12 call filters and data filters in **Filter Setup** and even link them in a serial manner. Each filter set is composed by 7 filter rules, which can be further defined. After that, in **General Setup** you may specify one set for call filter and one set for data filter to execute first.



4.5.4 DoS Defense

As a sub-functionality of IP Filter/Firewall, there are 15 types of detect/ defense function in the **DoS Defense** setup. The DoS Defense functionality is disabled for default.

Click Firewall and click DoS Defense to open the setup page.

Firewal	>>	DoS	defense	Setup
	-			

DoS defense Setup			
Enable DoS Defense			
Enable SYN flood defense	Threshold	50	packets / sec
	Timeout	10	sec
Enable UDP flood defense	Threshold	150	packets / sec
	Timeout	10	sec
Enable ICMP flood defense	Threshold	50	packets / sec
	Timeout	10	sec
Enable Port Scan detection	Threshold	150	packets / sec
Block IP options	🔲 Block TCP flag	scan	
Block Land	📃 Block Tear Droj	o	
Block Smurf	📃 Block Ping of D	eath	
🔲 Block trace route	📃 Block ICMP frag	gment	
🔲 Block SYN fragment	🔲 Block Unknown	Protocol	
📃 Block Fraggle Attack			
Enable DoS defense function to preve crackers.	nt the attacks fr	om hacker	or 🔨
L			

ОК	Clear All	Cancel

Enable Dos Defense	Check the box to activate the DoS Defense Functionality.
Enable SYN flood defense	Check the box to activate the SYN flood defense function. Once detecting the Threshold of the TCP SYN packets from the Internet has exceeded the defined value, the Vigor router will start to randomly discard the subsequent TCP SYN packets for a period defined in Timeout. The goal for this is prevent the TCP SYN packets' attempt to exhaust the limited-resource of Vigor router. By default, the threshold and timeout values are set to 50 packets per second and 10 seconds, respectively.
Enable UDP flood defense	Check the box to activate the UDP flood defense function. Once detecting the Threshold of the UDP packets from the Internet has exceeded the defined value, the Vigor router will start to randomly discard the subsequent UDP packets for a period defined in Timeout. The default setting for threshold and timeout are 150 packets per second and 10 seconds, respectively.
Enable ICMP flood defense	Check the box to activate the ICMP flood defense function. Similar to the UDP flood defense function, once if the Threshold of ICMP packets from Internet has exceeded the defined value, the router will discard the ICMP echo requests coming from the Internet. The default setting for threshold and timeout are 50 packets per second and 10 seconds, respectively.

Enable PortScan detection	Port Scan attacks the Vigor router by sending lots of packets to many ports in an attempt to find ignorant services would respond. Check the box to activate the Port Scan detection. Whenever detecting this malicious exploration behavior by monitoring the port-scanning Threshold rate, the Vigor router will send out a warning. By default, the Vigor router sets the threshold as 150 packets per second.
Block IP options	Check the box to activate the Block IP options function. The Vigor router will ignore any IP packets with IP option field in the datagram header. The reason for limitation is IP option appears to be a vulnerability of the security for the LAN because it will carry significant information, such as security, TCC (closed user group) parameters, a series of Internet addresses, routing messagesetc. An eavesdropper outside might learn the details of your private networks.
Block Land	Check the box to enforce the Vigor router to defense the Land attacks. The Land attack combines the SYN attack technology with IP spoofing. A Land attack occurs when an attacker sends spoofed SYN packets with the identical source and destination addresses, as well as the port number to victims.
Block Smurf	Check the box to activate the Block Smurf function. The Vigor router will ignore any broadcasting ICMP echo request.
Block trace router	Check the box to enforce the Vigor router not to forward any trace route packets.
Block SYN fragment	Check the box to activate the Block SYN fragment function. The Vigor router will drop any packets having SYN flag and more fragment bit set.
Block Fraggle Attack	Check the box to activate the Block fraggle Attack function. Any broadcast UDP packets received from the Internet is blocked. Activating the DoS/DDoS defense functionality might block some legal packets. For example, when you activate the fraggle attack defense, all broadcast UDP packets coming from the Internet are blocked. Therefore, the RIP packets from the Internet might be dropped.
Block TCP flag scan	Check the box to activate the Block TCP flag scan function. Any TCP packet with anomaly flag setting is dropped. Those scanning activities include <i>no flag scan</i> , <i>FIN without ACK scan</i> , <i>SYN FINscan</i> , <i>Xmas scan</i> and <i>full Xmas scan</i> .
Block Tear Drop	Check the box to activate the Block Tear Drop function. Many machines may crash when receiving ICMP datagrams (packets) that exceed the maximum length. To avoid this type of attack, the Vigor router is designed to be capable of discarding any fragmented ICMP packets with a length greater than 1024 octets.
Block Ping of Death	Check the box to activate the Block Ping of Death function. This attack involves the perpetrator sending overlapping packets to the target hosts so that those target hosts will hang once they re-construct the packets. The Vigor routers will block any packets realizing this attacking activity.
Block ICMP Fragment	Check the box to activate the Block ICMP fragment function. Any ICMP packets with more fragment bit set are dropped.



Block Unknown Protocol	Check the box to activate the Block Unknown Protocol function. Individual IP packet has a protocol field in the datagram header to indicate the protocol type running over the upper layer. However, the protocol types greater than 100 are reserved and undefined at this time. Therefore, the router should have ability to detect and reject this kind of packets.
Warning Messages	We provide Syslog function for user to retrieve message from Vigor router. The user, as a Syslog Server, shall receive the report sending from Vigor router which is a Syslog Client.
	All the warning messages related to DoS Defense will be sent to user

All the warning messages related to **DoS Defense** will be sent to user and user can review it through Syslog daemon. Look for the keyword **DoS** in the message, followed by a name to indicate what kind of attacks is detected.

System Maintenance >> SysLog / Mail Alert Setup

ysLog Access S	etun		Mail Alert Setup	
Enable	ocup		🗹 Enable	Send a test e-mail
erver IP Address	19	2.168.1.5	SMTP Server	
			Mail To	
estination Port	51-	ł		
hable syslog mes:	sage:		Return-Path	
Firewall Log			Authentication	
VPN Log			User Name	
User Access	Log		Password	
Call Log			Enable E-Mail Alert: DoS Attack	
WAN Log			M-P2P	
🗹 Router/DSL i	nformatior		MIM-P2P	
OrayTek Syslog 3.7.0				
ontrols				
ontrols	192.168.	Ga	teway IP (Fixed) TX Packets	TX Rate
		1.1		TX Rate
	Vigo	'Series Ga	teway IP (Fixed) TX Packets	
AN Status	Vigo RX F	Series Ga	teway IP (Fixed) TX Packets 172.16.3.4 343	3
AN Status TX Packets 4175	RX F	Vackets	teway IP (Fixed) TX Packets 172.16.3.4 343 WAN IP (Fixed) RX Packets 172.16.3.229 2558	3 RX Rate 126
AN Status TX Packets 4175 rewall Log VPN Log U	RX F RX F Ser Access Log	Call Log WAN Log Others 1	teway IP (Fixed) TX Packets 172.16.3.4 343 WAN IP (Fixed) RX Packets	3 RX Rate 126
AN Status TX Packets 4175 rewall Log VPN Log U Time	Ser Access Log	Gadeets Call Log WAN Log Others 1 Message	teway IP (Fixed) TX Packets 172.16.3.4 343 WAN IP (Fixed) RX Packets 172.16.3.229 2558 Network Information Net State Traffic Gro	RX Rate 126
AN Status TX Packets 4175 rewall Log VPN Log U	RX F RX F Ser Access Log	Call Log WAN Log Others 1 Message DoS syn, flood Block(10) 192.1	teway IP (Fixed) TX Packets 172.16.3.4 343 WAN IP (Fixed) RX Packets 172.16.3.229 2558	3 RX Rate 126 wh
AN Status TX Packets 4175 rewall Log VPN Log U Jan 1000042	RX F RX F Ser Access Log Host Vigor	Call Log WAN Log Others 1 Message DoS syn, flood Block(10) 192.1	teway IP (Fixed) TX Packets 172.16.3.4 343 WAN IP (Fixed) RX Packets 172.16.3.229 2558 Network Information Net State Traffic Gra 68.1.115,10605 -> 192.168.1.1,23 PR 6 (hep	3 RX Rate 126 wh
AN Status TX Packets 4175 rewall Log VPN Log U Jan 1000042	RX F RX F Ser Access Log Host Vigor	Call Log WAN Log Others 1 Message DoS syn, flood Block(10) 192.1	teway IP (Fixed) TX Packets 172.16.3.4 343 WAN IP (Fixed) RX Packets 172.16.3.229 2558 Network Information Net State Traffic Gra 68.1.115,10605 -> 192.168.1.1,23 PR 6 (hep	3 RX Rate 126 wh
AN Status TX Packets 4175 rewall Log VPN Log U Jan 1000042	RX F RX F Ser Access Log Host Vigor	Call Log WAN Log Others 1 Message DoS syn, flood Block(10) 192.1	teway IP (Fixed) TX Packets 172.16.3.4 343 WAN IP (Fixed) RX Packets 172.16.3.229 2558 Network Information Net State Traffic Gra 68.1.115,10605 -> 192.168.1.1,23 PR 6 (hep	3 RX Rate 126 wh
AN Status TX Packets 4175 rewall Log VPN Log U Jan 1000042	RX F RX F Ser Access Log Host Vigor	Call Log WAN Log Others 1 Message DoS syn, flood Block(10) 192.1	teway IP (Fixed) TX Packets 172.16.3.4 343 WAN IP (Fixed) RX Packets 172.16.3.229 2558 Network Information Net State Traffic Gra 68.1.115,10605 -> 192.168.1.1,23 PR 6 (hep	3 RX Rate 126 wh
AN Status TX Packets 4175 rewall Log VPN Log U Jan 1000042	RX F RX F Ser Access Log Host Vigor	Call Log WAN Log Others 1 Message DoS syn, flood Block(10) 192.1	teway IP (Fixed) TX Packets 172.16.3.4 343 WAN IP (Fixed) RX Packets 172.16.3.229 2558 Network Information Net State Traffic Gra 68.1.115,10605 -> 192.168.1.1,23 PR 6 (hep	3 RX Rate 126 wh
AN Status TX Packets 4175 rewall Log VPN Log U Jan 1000042	RX F RX F Ser Access Log Host Vigor	Call Log WAN Log Others 1 Message DoS syn, flood Block(10) 192.1	teway IP (Fixed) TX Packets 172.16.3.4 343 WAN IP (Fixed) RX Packets 172.16.3.229 2558 Network Information Net State Traffic Gra 68.1.115,10605 -> 192.168.1.1,23 PR 6 (hep	3 RX Rate 126 wh
AN Status TX Packets 4175 rewall Log VPN Log U Jan 1000042	RX F RX F Ser Access Log Host Vigor	Call Log WAN Log Others 1 Message DoS syn, flood Block(10) 192.1	teway IP (Fixed) TX Packets 172.16.3.4 343 WAN IP (Fixed) RX Packets 172.16.3.229 2558 Network Information Net State Traffic Gra 68.1.115,10605 -> 192.168.1.1,23 PR 6 (hep	3 RX Rate 126 wh
AN Status TX Packets 4175 rewall Log VPN Log U Jan 1000042	RX F RX F Ser Access Log Host Vigor	Call Log WAN Log Others 1 Message DoS syn, flood Block(10) 192.1	teway IP (Fixed) TX Packets 172.16.3.4 343 WAN IP (Fixed) RX Packets 172.16.3.229 2558 Network Information Net State Traffic Gra 68.1.115,10605 -> 192.168.1.1,23 PR 6 (hep	3 RX Rate 126 wh
AN Status TX Packets 4175 rewall Log VPN Log U Jan 1000042	RX F RX F Ser Access Log Host Vigor	Call Log WAN Log Others 1 Message DoS syn, flood Block(10) 192.1	teway IP (Fixed) TX Packets 172.16.3.4 343 WAN IP (Fixed) RX Packets 172.16.3.229 2558 Network Information Net State Traffic Gra 68.1.115,10605 -> 192.168.1.1,23 PR 6 (hep	3 RX Rate 126 wh
AN Status TX Packets 4175 rewall Log VPN Log U Jan 1000042	RX F RX F Ser Access Log Host Vigor	Call Log WAN Log Others 1 Message DoS syn, flood Block(10) 192.1	teway IP (Fixed) TX Packets 172.16.3.4 343 WAN IP (Fixed) RX Packets 172.16.3.229 2558 Network Information Net State Traffic Gra 68.1.115,10605 -> 192.168.1.1,23 PR 6 (hep	3 RX Rate 126 wh
AN Status TX Packets 4175 rewall Log VPN Log U Jan 1000042	RX F RX F Ser Access Log Host Vigor	Call Log WAN Log Others 1 Message DoS syn, flood Block(10) 192.1	teway IP (Fixed) TX Packets 172.16.3.4 343 WAN IP (Fixed) RX Packets 172.16.3.229 2558 Network Information Net State Traffic Gra 68.1.115,10605 -> 192.168.1.1,23 PR 6 (hep	3 RX Rate 126 wh
AN Status TX Packets 4175 rewall Log VPN Log U Jan 1000042	RX F RX F Ser Access Log Host Vigor	Call Log WAN Log Others 1 Message DoS syn, flood Block(10) 192.1	teway IP (Fixed) TX Packets 172.16.3.4 343 WAN IP (Fixed) RX Packets 172.16.3.229 2558 Network Information Net State Traffic Gra 68.1.115,10605 -> 192.168.1.1,23 PR 6 (hep	3 RX Rate 126 wh

4.6 Objects Settings

For IPs in a range and service ports in a limited range usually will be applied in configuring router's settings, therefore we can define them with *objects* and bind them with *groups* for using conveniently. Later, we can select that object/group that can apply it. For example, all the IPs in the same department can be defined with an IP object (a range of IP address).

Objects Setting
* IP Object
Service Type Object
Service Type Group
Keyword Object
 File Extension Object
T IM Object
P2P Object

4.6.1 IP Object

You can set up to 192 sets of IP Objects with different conditions.

Index	Name	Index	Name
<u>1.</u>		<u>17.</u>	
<u>2.</u>		<u>18.</u>	
<u>3.</u>		<u>19.</u>	
<u>4.</u>		<u>20.</u>	
<u>5.</u>		<u>21.</u>	
<u>6.</u>		<u>22.</u>	
<u>7.</u>		<u>23.</u>	
<u>8.</u>		<u>24.</u>	
<u>9.</u>		<u>25.</u>	
<u>10.</u>		<u>26.</u>	
<u>11.</u>		<u>27.</u>	
<u>12.</u>		<u>28.</u>	
<u>13.</u>		<u>29.</u>	
<u>14.</u>		<u>30.</u>	
<u>15.</u>		<u>31.</u>	
<u>16.</u>		<u>32.</u>	

Objects Setting >> IP Object

Set to Factory Default Cle

Clear all profiles.

Click the number under Index column for settings in detail.

Objects Setting >> IP Object

Name:	RD Department
Interface:	Any V
Address Type:	Range Address 👻
Start IP Address:	192.168.1.64
End IP Address:	192.168.1.75
Subnet Mask:	0.0.0
Invert Selection:	
Jame	OK Clear Cancel Type a name for this profile. Maximum 15 characters are allowed.
nterface	Choose a proper interface (WAN, LAN or Any).
	Interface: Any LAN WAN For example, the Direction setting in Edit Filter Rule will a you specify IP or IP range for WAN or LAN or any IP address
	If you choose LAN as the Interface here, and choose LAN a the direction setting in Edit Filter Rule , then all the IP addresses specified with LAN interface will be opened for yo to choose in Edit Filter Rule page.
Address Type	 Determine the address type for the IP address. Select Single Address if this object contains one IP address only. Select Range Address if this object contains several IPs with a range. Select Subnet Address if this object contains one subnet for
	address. Select Any Address if this object contains any IP address.
Start IP Address	Type the start IP address for Single Address type.
End IP Address	Type the end IP address if the Range Address type is selected
Subnet Mask	Type the subnet mask if the Subnet Address type is selected.

Below is an example of IP objects settings.

Objects Setting >> IP Object

IP Object	Profiles:
Index	Name
<u>1.</u>	RD Department
<u>2.</u>	Finanical Dept.
<u>3.</u>	HR Department
<u>4.</u>	

4.5.2 IP Group

This page allows you to bind several IP objects into one IP group.

P Group Table:			Set to Factory Default
Index	Name	Index	Name
<u>1.</u>		<u>17.</u>	
<u>2.</u>		<u>18.</u>	
<u>3.</u>		<u>19.</u>	
<u>4.</u>		<u>20.</u>	
<u>5.</u>		<u>21.</u>	
<u>6.</u>		<u>22.</u>	
<u>7.</u>		<u>23.</u>	
<u>8.</u>		<u>24.</u>	
<u>9.</u>		<u>25.</u>	
<u>10.</u>		<u>26.</u>	
<u>11.</u>		<u>27.</u>	
<u>12.</u>		<u>28.</u>	
<u>13.</u>		<u>29.</u>	
<u>14.</u>		<u>30.</u>	
<u>15.</u>		<u>31.</u>	
<u>16.</u>		<u>32.</u>	

Objects Setting >> IP Group

Set to Factory Default Clear all profiles.

Click the number under Index column for settings in detail.

Objects Setting >> IP Group

Profile Index : 1		
Name:		
Interface:	Any 💌	
Available IP Objects	Selected IP Objects	
1-RD Department 2-Finanical Dept. 3-HR Department	» «	
(OK Clear Cancel	
Name	Type a name for this profile. Maximum 15 characters are allowed.	
Interface	Choose WAN, LAN or Any to display all the available IP objects with the specified interface.	
Available IP Objects	All the available IP objects with the specified interface chosen above will be shown in this box.	
Selected IP Objects	Click >> button to add the selected IP objects in this box.	

4.6.3 Service Type Object

You can set up to 96 sets of Service Type Objects with different conditions.

Index	Name	Index	Name
<u>1.</u>		<u>17.</u>	
<u>2.</u>		<u>18.</u>	
<u>3.</u>		<u>19.</u>	
<u>4.</u>		<u>20.</u>	
<u>5.</u>		<u>21.</u>	
<u>6.</u>		<u>22.</u>	
<u>7.</u>		<u>23.</u>	
<u>8.</u>		<u>24.</u>	
<u>9.</u>		<u>25.</u>	
<u>10.</u>		<u>26.</u>	
<u>11.</u>		<u>27.</u>	
<u>12.</u>		<u>28.</u>	
<u>13.</u>		<u>29.</u>	
<u>14.</u>		<u>30.</u>	
<u>15.</u>		<u>31.</u>	
<u>16.</u>		<u>32.</u>	

Set to Factory Default Clear all profiles.

Click the number under Index column for settings in detail.

Objects Setting >> Service Type Object Setup

Name	www
Protocol	TCP 🖌 6
Source Port	= 🖌 1 ~ 65535
Destination Port	= 🖌 1 ~ 65535

Name

Type a name for this profile.

Protocol

Specify the protocol(s) which this profile will apply to.

тср 🖌	
Any	
ICMP	
IGMP	
TCP	
UDP	
TCP/UDP	
Other	

Source/Destination Port Source Port and the Destination Port column are available for TCP/UDP protocol. It can be ignored for other protocols. The filter rule will filter out any port number.



(=) - when the first and last value are the same, it indicates one port; when the first and last values are different, it indicates a range for the port and available for this profile.
(!=) - when the first and last value are the same, it indicates all the ports except the port defined here; when the first and last values are different, it indicates that all the ports except the range defined here are available for this service type.
(>) - the port number greater than this value is available.
(<) - the port number less than this value is available for this profile.

Below is an example of service type objects settings.

Objects Setting >> Service Type Object

Service Type Object Profiles:

Index	Name
<u>1.</u>	SIP
<u>2.</u>	RTP
3.	

4.5.4 Service Type Group

This page allows you to bind several service types into one group.

Objects Setting >> Service Type Group

ervice Type Group Table:			Set to Factory Default		
Group	Name	Group	Name		
<u>1.</u>		<u>17.</u>			
<u>2.</u>		<u>18.</u>			
<u>3.</u>		<u>19.</u>			
<u>4.</u>		<u>20.</u>			
<u>5.</u>		<u>21.</u>			
<u>6.</u>		<u>22.</u>			
<u>7.</u>		<u>23.</u>			
<u>8.</u>		<u>24.</u>			
<u>9.</u>		<u>25.</u>			
<u>10.</u>		<u>26.</u>			
<u>11.</u>		<u>27.</u>			
<u>12.</u>		<u>28.</u>			
<u>13.</u>		<u>29.</u>			
<u>14.</u>		<u>30.</u>			
<u>15.</u>		<u>31.</u>			
<u>16.</u>		<u>32.</u>			

Set to Factory Default

Clear all profiles.

Click the number under Index column for settings in detail.



Objects Setting >> Service Type Group Setup

Name:	VoIP
Available Service Ty	pe Objects Selected Service Type Objects
1-SIP 2-RTP	
	OK Clear Cancel
Jame	Type a name for this profile.
Available Service Type Dbjects	All the available service objects that you have added on Objects Setting>>Service Type Object will be shown in this box.
Selected Service Type Objects	Click >> button to add the selected IP objects in this box.

4.6.5 Keyword Object

You can set 200 keyword object profiles for choosing as black /white list in CSM >>URL Web Content Filter Profile.

Index	Name	Index	Name
<u>1.</u>		<u>17.</u>	
<u>2.</u>		<u>18.</u>	
<u>3.</u>		<u>19.</u>	
<u>4.</u>		<u>20.</u>	
<u>5.</u>		<u>21.</u>	
<u>6.</u>		<u>22.</u>	
<u>7.</u>		<u>23.</u>	
<u>8.</u>		<u>24.</u>	
<u>9.</u>		<u>25.</u>	
<u>10.</u>		<u>26.</u>	
<u>11.</u>		<u>27.</u>	
<u>12.</u>		<u>28.</u>	
<u>13.</u>		<u>29.</u>	
<u>14.</u>		<u>30.</u>	
<u>15.</u>		<u>31.</u>	
<u>16.</u>		<u>32.</u>	

Objects Setting >> Keyword Object

Set to Factory Default

Clear all profiles.

Click the number under Index column for setting in detail.

Objects Setting >> Keyword Object Setup

Profile Index : 1	
Name	
Contents	(Max 63 characters)
	OK Clear Cancel
Name	Type a name for this profile, e.g., game.
Contents	Type the content for such profile. For example, type <i>gambling</i> as Contents. When you browse the webpage, the page with gambling information will be watched out and be passed/blocked based on the configuration on Firewall settings

4.5.6 Keyword Group

This page allows you to bind several keyword objects into one group. The keyword groups set here will be chosen as black /white list in **CSM >>URL Web Content Filter Profile**.

eyword Group T			Set to Factory Defau
Index	Name	Index	Name
<u>1.</u>		<u>17.</u>	
<u>2.</u>		<u>18.</u>	
<u>3.</u>		<u>19.</u>	
<u>4.</u>		<u>20.</u>	
<u>5.</u>		<u>21.</u>	
<u>6.</u>		<u>22.</u>	
<u>7.</u>		<u>23.</u>	
<u>8.</u>		<u>24.</u>	
<u>9.</u>		<u>25.</u>	
<u>10.</u>		<u>26.</u>	
<u>11.</u>		<u>27.</u>	
<u>12.</u>		<u>28.</u>	
<u>13.</u>		<u>29.</u>	
<u>14.</u>		<u>30.</u>	
<u>15.</u>		<u>31.</u>	
16.		<u>32.</u>	

Objects Setting >> Keyword Group

Set to Factory Default Clear all profiles.

Click the number under Index column for setting in detail.

Objects Setting >> Keyword Group Setup

Profile Index : 1	
Name:	
Available Keyword Objects	Selected Keyword Objects(Max 16 Objects)
1-Keyword-1 2-keyword-2	» «
	OK Clear Cancel
Name	Type a name for this group.
Available Keyword Objects	You can gather keyword objects from Keyword Object page within one keyword group. All the available Keyword objects that you have created will be shown in this box.
Selected Keyword Objects	Click button to add the selected Keyword objects in this box.

4.6.7 File Extension Object

This page allows you to set eight profiles which will be applied in **CSM>>URL Content Filter**. All the files with the extension names specified in these profiles will be processed according to the chosen action.

Profile 1 with name of "default" is the default profile, some files with the file extensions specified in this profile will be ignored and not be scanned by Vigor router.

)bjects Setting>	File Extension Object	t	
File Extension Ob	ject Profiles:		Set to Factory Defau
Profile	Name	Profile	Name
<u>1.</u>		<u>5.</u>	
<u>2.</u>		<u>6.</u>	
<u>3.</u>		<u>7.</u>	
<u>4.</u>		<u>8.</u>	

Set to Factory Default

Clear all profiles.

Click the number under Profile column for configuration in details.

Objects Setting >> File Extension Object Setup

Profile Index: 1		Profile	Name:				
Categories			Fi	le Extensio	ons		
Image Select All Clear All	.bmp .pct	□.dib □.pcx	.gif	.jpeg . .pict	.jpg .jpg	.jpg2 .tif	□.jp2 □.tiff
Video Select All Clear All	□.asf □.qt	🗌 .avi 🗌 .rm	.mov .wmv	.mpe .3gp	🗌 .mpeg 🗌 .3gpp	.mpg .3gpp2	□.mp4 □.3g2
Audio Select All Clear All	□.aac □.ra	□.aiff □.ram	.au .vox	□.mp3 □.wav	□.m4a □.wma	□.m4p	🗆 .ogg
Java Select All Clear All	□.class □.jse	□.jad □.jsp	□.jar □.jtk	🗌 .jav	🗌 .java	🗌 .jcm	🗆 .js
ActiveX Select All Clear All	🗌 . alx 🗋 . viv	.apb .vrm	🗖 . axs	.ocx	🗌 . olb	.ole	🗖 . tlb
Compression Select All Clear All	.ace .rar	□.arj □.sit	□.bzip2 □.zip	.bz2	🗌 .cab	.gz	🗆 . gzip
Executation Select All Clear All	.bas .scr	🗌 .bat	.com	.exe	.inf	🗌 .pif	.reg
-		OK	Clear	Canc	el		

Profile Name

Type a name for this profile.

Type a name for such profile and check all the items of file extension that will be processed in the router. Finally, click **OK** to save this profile.

4.6.8 IM Object

This page allows you to set 32 profiles for Instant Messenger. These profiles will be applied in **CSM>>IM/P2P Filter Profile** for filtering.

M Profile Table:	Bie weer	Du-fil-	Set to Factory Defaul
Profile	Name	Profile	Name
<u>1.</u>		<u>17.</u>	
<u>2.</u>		<u>18.</u>	
<u>3.</u>		<u>19.</u>	
<u>4.</u>		<u>20.</u>	
<u>5.</u>		<u>21.</u>	
<u>6.</u>		<u>22.</u>	
<u>7.</u>		<u>23.</u>	
<u>8.</u>		<u>24.</u>	
<u>9.</u>		<u>25.</u>	
<u>10.</u>		<u>26.</u>	
<u>11.</u>		<u>27.</u>	
<u>12.</u>		<u>28.</u>	
<u>13.</u>		<u>29.</u>	
<u>14.</u>		<u>30.</u>	
<u>15.</u>		<u>31.</u>	
<u>16.</u>		32.	

Objects Setting >> IM Object Profile

Set to Factory Default Clear all profiles.

Click the number under Profile column for configuration in details. There are several types of Instant Messenger (IM) provided here for you to choose to disallow people using. Simple check the box (es) and then click **OK**. Later, in the **CSM>>IM/P2P Filter Profile** page, you can use **IM Object** drop down list to choose the proper profile configured here as the standard for the host(s) to follow.

Objects	Setting	>> IM	Objec	t Profile
---------	---------	-------	-------	-----------

Profile Index: 1					
Profile Name:					
	Select All]			
Check for Disallov	v.	J			
	I	M Application			VoIP
					Skype
MSN	🗌 YahooIM	AIM	ICQ		🗌 Kubao
□QQ	🗌 iChat	Jabber/Goo	gleTalk 🔲 Googl	eChat	Gizmo
					SIP
	W	eb IM (* = more	than one addres	s)	
	<u>eMessenger</u>	<u>WebMSN</u>	meebo*	<u>eBuddy</u>	ILoveIM*
WebIM URLs	ICQ Java*	ICQ Flash*	goowy*	<u>IMhaha*</u>	<u>getMessenger</u>
	IMUnitive*	Wablet*	mabber*	MSN2GO*	<u>KoollM</u>
	MessengerFX*	MessengerAdicto	os <u>WebYahoolM</u>		
		OK Cle	ar Cancel		

Profile Name

Type a name for this profile.



Type a name for such profile and check all the items that not allowed to be used in the host. Finally, click **OK** to save this profile.

4.6.9 P2P Object

This page allows you to set 32 profiles for peer-to-peer application. These profiles will be applied in **CSM>>IM/P2P Filter Profile** for filtering.

2P Profile Table	•		Set to Factory Default
Profile	Name	Profile	Name
<u>1.</u>		<u>17.</u>	
<u>2.</u>		<u>18.</u>	
<u>3.</u>		<u>19.</u>	
<u>4.</u>		<u>20.</u>	
<u>5.</u>		<u>21.</u>	
<u>6.</u>		<u>22.</u>	
<u>7.</u>		<u>23.</u>	
<u>8.</u>		<u>24.</u>	
<u>9.</u>		<u>25.</u>	
<u>10.</u>		<u>26.</u>	
<u>11.</u>		<u>27.</u>	
<u>12.</u>		<u>28.</u>	
<u>13.</u>		<u>29.</u>	
<u>14.</u>		<u>30.</u>	
<u>15.</u>		<u>31.</u>	
<u>16.</u>		<u>32.</u>	

Objects Setting >> P2P Object Profile

Set to Factory Default Clear all profiles.

Click the number under Profile column for configuration in details. There are several items for P2P protocols provided here for you to choose to disallow people using. Simple check the box (es) and then click **OK**. Later, in the **CSM>>IM/P2P Filter Profile** page, you can use **P2P Object** drop down list to choose the proper profile configured here as the standard for the host(s) to follow.

Profile Index: 1 Profile Name: Check for Disallow: Applications Protocol SoulSeek SoulSeek eDonkey eDonkey, eMule, Shareaza KazaA, BearShare, iMesh 🗌 FastTrack OpenFT KCeasy, FilePipe 🗌 Gnutella BearShare, Limewire, Shareaza, Foxy Lopster, XNap, WinLop 🗌 OpenNap BitTorrent BitTorrent, BitSpirit, BitComet 🗌 Winny Winny, WinMX, Share ΟK Clear Cancel

Objects Setting >> P2P Object Profile

Profile Name

Type a name for this profile.



Type a name for such profile and check all the protocols that not allowed to be used in the host. Finally, click **OK** to save this profile.

4.6.10 Misc Object

This page allows you to set 32 profiles for miscellaneous applications. These profiles will be applied in **CSM>>IM/P2P Filter Profile** for filtering.

Misc Profile Table	:		Set to Factory Default
Profile	Name	Profile	Name
<u>1.</u>		<u>17.</u>	
<u>2.</u>		<u>18.</u>	
<u>3.</u>		<u>19.</u>	
<u>4.</u>		<u>20.</u>	
<u>5.</u>		<u>21.</u>	
<u>6.</u>		<u>22.</u>	
<u>7.</u>		<u>23.</u>	
<u>8.</u>		<u>24.</u>	
<u>9.</u>		<u>25.</u>	
<u>10.</u>		<u>26.</u>	
<u>11.</u>		<u>27.</u>	
<u>12.</u>		<u>28.</u>	
<u>13.</u>		<u>29.</u>	
<u>14.</u>		<u>30.</u>	
<u>15.</u>		<u>31.</u>	
<u>16.</u>		<u>32.</u>	

Objects Setting >> Misc Object Profile

Set to Factory Default Clear all profiles.

Objects Setting >> Misc Object Profile

Click the number under Profile column for configuration in details. Applications for tunneling and streaming are listed in the page for you to choose to disallow people using. Simple check the box (es) and then click **OK**. Later, in the **CSM>>IM/P2P Filter Profile** page, you can use **Misc Object** drop down list to choose the proper profile configured here as the standard for the host(s) to follow.

rofile Index: 1				
rofile Name:				
heck for Disallo	w: Select All			
		Streaming		
MMS	RTSP	TVAnts	PPStream	PPlive
EeiDian	UUSee	NSPlayer	PCAST	TVKoo
SopCast	UDLiveX	TVUPlayer	MySee	🗌 Joost
FlashVideo	SilverLight	Slingbox	QVOD	

Profile Name

Type a name for this profile.

Type a name for such profile and check all the protocols that not allowed to be used in the host. Finally, click **OK** to save this profile.



4.7 CSM Profile

Content Security Management (CSM)

CSM is an abbreviation of **Content Security Management** which is used to control IM/P2P usage, filter the web content and URL content to reach a goal of security management.

As the popularity of all kinds of instant messenger application arises, communication cannot become much easier. Nevertheless, while some industry may leverage this as a great tool to connect with their customers, some industry may take reserve attitude in order to reduce employee misusage during office hour or prevent unknown security leak. It is similar situation for corporation towards peer-to-peer applications since file-sharing can be convenient but insecure at the same time. To address these needs, we provide CSM functionality.

IM/P2P Filter

As the popularity of all kinds of instant messenger application arises, communication cannot become much easier. Nevertheless, while some industry may leverage this as a great tool to connect with their customers, some industry may take reserve attitude in order to reduce employee misusage during office hour or prevent unknown security leak. It is similar situation for corporation towards peer-to-peer applications since file-sharing can be convenient but insecure at the same time. To address these needs, we provide CSM functionality.

URL Content Filter

To provide an appropriate cyberspace to users, Vigor router equips with **URL Content Filter** not only to limit illegal traffic from/to the inappropriate web sites but also prohibit other web feature where malicious code may conceal.

Once a user type in or click on an URL with objectionable keywords, URL keyword blocking facility will decline the HTTP request to that web page thus can limit user's access to the website. You may imagine **URL Content Filter** as a well-trained convenience-store clerk who won't sell adult magazines to teenagers. At office, **URL Content Filter** can also provide a job-related only environment hence to increase the employee work efficiency. How can URL Content Filter work better than traditional firewall in the field of filtering? Because it checks the URL strings or some of HTTP data hiding in the payload of TCP packets while legacy firewall inspects packets based on the fields of TCP/IP headers only.

On the other hand, Vigor router can prevent user from accidentally downloading malicious codes from web pages. It's very common that malicious codes conceal in the executable objects, such as ActiveX, Java Applet, compressed files, and other executable files. Once downloading these types of files from websites, you may risk bringing threat to your system. For example, an ActiveX control object is usually used for providing interactive web feature. If malicious code hides inside, it may occupy user's system.

Web Content Filter

We all know that the content on the Internet just like other types of media may be inappropriate sometimes. As a responsible parent or employer, you should protect those in your trust against the hazards. With Web filtering service of the Vigor router, you can protect your business from common primary threats, such as productivity, legal liability, network and security threats. For parents, you can protect your children from viewing adult websites or chat rooms.

Once you have activated your Web Filtering service in Vigor router and chosen the categories of website you wish to restrict, each URL address requested (e.g.www.bbc.co.uk) will be checked against our server database. This database is updated as frequent as daily by a global team of Internet researchers. The server will look up the URL and return a category to your router. Your



Vigor router will then decide whether to allow access to this site according to the categories you have selected. Please note that this action will not introduce any delay in your Web surfing because each of multiple load balanced database servers can handle millions of requests for categorization.

Note: The priority of URL Content Filter is higher than Web Content Filter.



4.7.1 IM/P2P Filter Profile

CSM >> IM/P2P Filter Profile

You can define policy profiles for different policy of IM (Instant Messenger)/P2P (Peer to Peer) application. CSM profile can be used in Filter Setup page.

Profile	Name	Profile	Name
<u>1.</u>		<u>17.</u>	
<u>2.</u>		<u>18.</u>	
<u>3.</u>		<u>19.</u>	
<u>4.</u>		<u>20.</u>	
<u>5.</u>		<u>21.</u>	
<u>6.</u>		<u>22.</u>	
<u>7.</u>		<u>23.</u>	
<u>8.</u>		<u>24.</u>	
<u>9.</u>		<u>25.</u>	
<u>10.</u>		<u>26.</u>	
<u>11.</u>		<u>27.</u>	
<u>12.</u>		<u>28.</u>	
<u>13.</u>		<u>29.</u>	
<u>14.</u>		<u>30.</u>	
<u>15.</u>		<u>31.</u>	
<u>16.</u>		<u>32.</u>	

Set to Factory Default Clear all profiles.

Click the number under Index column for settings in detail.

Profile Index: 1	
Profile Name:	
IM Object	None 💌
P2P Object	None
Misc Object	None 💌
Misc Object	None Y

Profile Name

Type a name for the CSM profile.

Each profile can contain three objects settings, IM Object, P2P Object and Misc Object. Such profile can be applied in the **Firewall>>General Setup** and **Firewall>>Filter Setup** pages as the standard for the host(s) to follow.

4.7.2 URL Content Filter Profile

To provide an appropriate cyberspace to users, Vigor router equips with **URL Content Filter** not only to limit illegal traffic from/to the inappropriate web sites but also prohibit other web feature where malicious code may conceal.

Once a user type in or click on an URL with objectionable keywords, URL keyword blocking facility will decline the HTTP request to that web page thus can limit user's access to the website. You may imagine **URL Content Filter** as a well-trained convenience-store clerk who won't sell adult magazines to teenagers. At office, **URL Content Filter** can also provide a job-related only environment hence to increase the employee work efficiency. How can URL Content Filter work better than traditional firewall in the field of filtering? Because it checks the URL strings or some of HTTP data hiding in the payload of TCP packets while legacy firewall inspects packets based on the fields of TCP/IP headers only.

On the other hand, Vigor router can prevent user from accidentally downloading malicious codes from web pages. It's very common that malicious codes conceal in the executable objects, such as ActiveX, Java Applet, compressed files, and other executable files. Once downloading these types of files from websites, you may risk bringing threat to your system. For example, an ActiveX control object is usually used for providing interactive web feature. If malicious code hides inside, it may occupy user's system.

For example, if you add key words such as "sex", Vigor router will limit web access to web sites or web pages such as "www.sex.com", "www.backdoor.net/images/sex/p_386.html". Or you may simply specify the full or partial URL such as "www.sex.com" or "sex.com".

Also the Vigor router will discard any request that tries to retrieve the malicious code.

Click CSM and click URL Content Filter Profile to open the profile setting page.

	Name	Profile	Name
<u>1.</u>		<u>5.</u>	
<u>2.</u>		<u>6.</u>	
<u>3.</u>		<u>7.</u>	
<u>4.</u>		<u>8.</u>	

CSM >> URL Content Filter Profile

ок

You can set eight profiles as URL content filter. Simply click the index number under Profile to open the following web page.



CSM >> URL Content Filter Profile

Profile Name:	
Priority:	Both : Pass Vone V
1.URL Acces	s Control
🗌 Enabl	e URL Access Control Prevent web access from IP address
Actio Pass	
2.Web Featu	ire
Enable Action Pass	e Restrict Web Feature n: Cookie Proxy <u>File Extension Profile:</u> None Y
	OK Clear Cancel
Profile Name	Type the name for such profile.
Priority	It determines the action that this router will apply. Both: Pass – The router will let all the packages that match with the conditions specified in URL Access Control and Web Feature below passing through. When you choose this setting, both configuration set in this page for URL Access Control and Web Feature will be inactive. Both:Block –The router will block all the packages that match with the conditions specified in URL Access Control and Web Feature

below. When you choose this setting, both configuration set in this page for URL Access Control and Web Feature will be inactive. **Either: URL Access Control First** – When all the packages matching with the conditions specified in URL Access Control and Web Feature below, such function can determine the priority for the actions executed. For this one, the router will process the packages with the conditions set below for URL first, then Web feature second. **Either: Web Feature First** –When all the packages matching with the conditions specified in URL Access Control and Web Feature below, such function can determine the priority for the actions executed. For this one, the router will process the packages with the conditions specified in URL Access Control and Web Feature below, such function can determine the priority for the actions executed. For this one, the router will process the packages with the conditions set below for web feature first, then URL second.



None – There is no log file will be recorded for this profile. Pass – Only the log about Pass will be recorded in Syslog. Block – Only the log about Block will be recorded in Syslog.

Vigor2110 Series User's Guide



All – All the actions (Pass and Block) will be recorded in Syslog.



URL Access ControlEnable URL Access Control - Check the box to activate URL
Access Control. Note that the priority for URL Access Control is
higher than Restrict Web Feature. If the web content match the
setting set in URL Access Control, the router will execute the action
specified in this field and ignore the action specified under Restrict
Web Feature.

Prevent web access from IP address - Check the box to deny any web surfing activity using IP address, such as http://202.6.3.2. The reason for this is to prevent someone dodges the URL Access Control. You must clear your browser cache first so that the URL content filtering facility operates properly on a web page that you visited before.

Action – This setting is available only when Either : URL Access Control First or Either : Web Feature First is selected. *Pass* -Allow accessing into the corresponding webpage with the keywords listed on the box below.

Block - Restrict accessing into the corresponding webpage with the keywords listed on the box below.

If the web pages do not match with the keyword set here, it will be processed with reverse action.





Group/Object Selections – The Vigor router provides several frames for users to define keywords and each frame supports multiple keywords. The keyword could be a noun, a partial noun, or a complete URL string. Multiple keywords within a frame are separated by space, comma, or semicolon. In addition, the maximal length of each frame is 32-character long. After specifying keywords, the Vigor router will decline the connection request to the website whose URL string matched to any user-defined keyword. It should be noticed that the more simplified the blocking keyword list, the more efficiently the Vigor router perform.

Object/Group Edit	None 🗸
Keyword Object	
or Keyword Object	None 🛩
or <u>Keyword Group</u>	None 🛩
or Keyword Group	None 💌
or Keyword Group	None 💌
or Keyword Group	None 💌
or Keyword Group	None 🛩
ОК	Close

Web FeatureEnable Restrict Web Feature - Check this box to make the
keyword being blocked or passed.

Action - This setting is available only when Either: URL Access Control First or Either : Web Feature Firs is selected. Pass allows accessing into the corresponding webpage with the keywords listed on the box below.

Pass - Allow accessing into the corresponding webpage with the keywords listed on the box below.

Block - Restrict accessing into the corresponding webpage with the keywords listed on the box below.

If the web pages do not match with the specified feature set here, it will be processed with reverse action.

Cookie - Check the box to filter out the cookie transmission from inside to outside world to protect the local user's privacy.

Proxy - Check the box to reject any proxy transmission. To control efficiently the limited-bandwidth usage, it will be of great value to provide the blocking mechanism that filters out the multimedia files downloading from web pages.

File Extension Profile – Choose one of the profiles that you configured in **Object Setting>> File Extension Objects** previously for passing or blocking the file downloading.

File Extension Profile: None





4.7.3 Web Content Filter Profile

We all know that the content on the Internet just like other types of media may be inappropriate sometimes. As a responsible parent or employer, you should protect those in your trust against the hazards. With Web filtering service of the Vigor router, you can protect your business from common primary threats, such as productivity, legal liability, network and security threats. For parents, you can protect your children from viewing adult websites or chat rooms.

Once you have activated your Web Filtering service in Vigor router and chosen the categories of website you wish to restrict, each URL address requested (e.g.www.bbc.co.uk) will be checked against our server database. This database is updated as frequent as daily by a global team of Internet researchers. The server will look up the URL and return a category to your router. Your Vigor router will then decide whether to allow access to this site according to the categories you have selected. Please note that this action will not introduce any delay in your Web surfing because each of multiple load balanced database servers can handle millions of requests for categorization.

Click CSM and click Web Content Filter Profile to open the profile setting page.

Profile	Name	Profile	Name
<u>1.</u>		<u>5.</u>	
<u>2.</u>		<u>6.</u>	
<u>3.</u>		<u>7.</u>	
<u>4.</u>		<u>8.</u>	
dministration M	essage (Max 255 charact	ters)	
<pre><body><center><</center></body></pre>	br>The requested We e contact your system	eb page has been block administrator for fur	-

CSM >> Web Content Filter Profile

You can set eight profiles as Web content filter. Simply click the index number under Profile to open the following web page.

CSM >> Web Content Filter Profile

Profile Name:			
Action : Block 💌 Groups	Categories	log : Block 💌	
Child Protection Select All Clear All	Chat Gambling Sex	Criminal Hacking Violence	Drugs/Alcohol Hate speech Weapons
Leisure Select All Clear All	Advertisements Games Hobbies Personals Sports	Entertainment Glamour Lifestyle Photo Searches Streaming Media	 Food Health Motor Vehicles Shopping Travel
Business Select All Clear All	Computing/Internet	☐ Finance ☐ Real Estate ☐ Search Engine	☐ Job Search/Career ☐ Reference ☐ Web Mail
Others Select All Clear All	 Education News Usenet news 	☐ Hosting sites ☐ Religion <mark>☐ uncategorised sites</mark>	☐ Kid Sites ☐ Sex Education
ction			onding webpage with the
	Block - restrict acc categories listed of If the web pages d	cessing into the corre- n the box below.	sponding webpage with specified feature set her
og	Pass – Only the lo Block – Only the l		-

For this section, please refer to **Web Content Filter** user's guide.



4.8 Bandwidth Management

Below shows the menu items for Bandwidth Management.

Bandwidth Management Sessions Limit Bandwidth Limit Onality of Service

4.8.1 Sessions Limit

A PC with private IP address can access to the Internet via NAT router. The router will generate the records of NAT sessions for such connection. The P2P (Peer to Peer) applications (e.g., BitTorrent) always need many sessions for procession and also they will occupy over resources which might result in important accesses impacted. To solve the problem, you can use limit session to limit the session procession for specified Hosts.

In the **Bandwidth Management** menu, click **Sessions Limit** to open the web page.

	🖲 Enable 🔘 Disable
	Default Max Sessions: 100
	Limitation List
	Index Start IP End IP Max Sessions
	Specific Limitation
	Start IP: End IP:
	Maximum Sessions:
	Add Edit Delete
ime Sc	hedule
Inc	lex(1-15) in <u>Schedule</u> Setup:,,,,,
No	te: Action and Idle Timeout settings will be ignored.

ΟK

Bandwidth Management >> Sessions Limit

To activate the function of limit session, simply click **Enable** and set the default session limit.

Enable	Click this button to activate the function of limit session.
Disable	Click this button to close the function of limit session.
Default session limit	Defines the default session number used for each computer in LAN.
Limitation List	Displays a list of specific limitations that you set on this web page.
Start IP	Defines the start IP address for limit session.
End IP	Defines the end IP address for limit session.

Maximum Sessions	Defines the available session number for each host in the specific range of IP addresses. If you do not set the session number in this field, the system will use the default session limit for the specific limitation you set for each index.
Add	Adds the specific session limitation onto the list above.
Edit	Allows you to edit the settings for the selected limitation.
Remove	Remove the selected settings existing on the limitation list.
Index (1-15) in Schedule Setup	You can type in four sets of time schedule for your request. All the schedules can be set previously in Application – Schedule web page and you can use the number that you have set in that web page.

4.8.2 Bandwidth Limit

The downstream or upstream from FTP, HTTP or some P2P applications will occupy large of bandwidth and affect the applications for other programs. Please use Limit Bandwidth to make the bandwidth usage more efficient.

In the **Bandwidth Management** menu, click **Bandwidth Limit** to open the web page.

Bandwidth Management >> Bandwidth Limit

Bandwidth Limit
○ Enable □ Apply to 2nd Subnet ④ Disable
Default TX Limit: 200 Kbps Default RX Limit: 800 Kbps
Limitation List
Index Start IP End IP TX limit RX limit
Specific Limitation
Start IP: End IP:
TX Limit: Kbps RX Limit: Kbps
Add Edit Delete
Time Schedule
Index(1-15) in <u>Schedule</u> Setup:,,,,
Note: Action and Idle Timeout settings will be ignored.
ОК

To activate the function of limit bandwidth, simply click **Enable** and set the default upstream and downstream limit.

	Click this button to activate the function of limit bandwidth. Apply to 2nd Subnet – Check this box to apply the bandwidth limit to the second subnet specified in LAN>>General Setup.
Disable	Click this button to close the function of limit bandwidth.



Default TX limit	Define the default speed of the upstream for each computer in LAN.
Default RX limit	Define the default speed of the downstream for each computer in LAN.
Limitation List	Display a list of specific limitations that you set on this web page.
Start IP	Define the start IP address for limit bandwidth.
End IP	Define the end IP address for limit bandwidth.
TX limit	Define the limitation for the speed of the upstream. If you do not set the limit in this field, the system will use the default speed for the specific limitation you set for each index.
RX limit	Define the limitation for the speed of the downstream. If you do not set the limit in this field, the system will use the default speed for the specific limitation you set for each index.
Add	Add the specific speed limitation onto the list above.
Edit	Allows you to edit the settings for the selected limitation.
Delete	Remove the selected settings existing on the limitation list.
Index (1-15) in Schedule Setup	You can type in four sets of time schedule for your request. All the schedules can be set previously in Application – Schedule web page and you can use the number that you have set in that web page.

4.8.3 Quality of Service

Deploying QoS (Quality of Service) management to guarantee that all applications receive the service levels required and sufficient bandwidth to meet performance expectations is indeed one important aspect of modern enterprise network.

One reason for QoS is that numerous TCP-based applications tend to continually increase their transmission rate and consume all available bandwidth, which is called TCP slow start. If other applications are not protected by QoS, it will detract much from their performance in the overcrowded network. This is especially essential to those are low tolerant of loss, delay or jitter (delay variation).

Another reason is due to congestions at network intersections where speeds of interconnected circuits mismatch or traffic aggregates, packets will queue up and traffic can be throttled back to a lower speed. If there's no defined priority to specify which packets should be discarded (or in another term "dropped") from an overflowing queue, packets of sensitive applications mentioned above might be the ones to drop off. How this will affect application performance?

There are two components within Primary configuration of QoS deployment:

- Classification: Identifying low-latency or crucial applications and marking them for high-priority service level enforcement throughout the network.
- Scheduling: Based on classification of service level to assign packets to queues and associated service types

The basic QoS implementation in Vigor routers is to classify and schedule packets based on the service type information in the IP header. For instance, to ensure the connection with the headquarter, a teleworker may enforce an index of QoS Control to reserve bandwidth for HTTPS connection while using lots of application at the same time.



One more larger-scale implementation of QoS network is to apply DSCP (Differentiated Service Code Point) and IP Precedence disciplines at Layer 3. Compared with legacy IP Precedence that uses Type of Service (ToS) field in the IP header to define 8 service classes, DSCP is a successor creating 64 classes possible with backward IP Precedence compatibility. In a QoS-enabled network, or Differentiated Service (DiffServ or DS) framework, a DS domain owner should sign a Service License Agreement (SLA) with other DS domain owners to define the service level provided toward traffic from different domains. Then each DS node in these domains will perform the priority treatment. This is called per-hop-behavior (PHB). The definition of PHB includes Expedited Forwarding (EF), Assured Forwarding (AF), and Best Effort (BE). AF defines the four classes of delivery (or forwarding) classes and three levels of drop precedence in each class.

Vigor routers as edge routers of DS domain shall check the marked DSCP value in the IP header of bypassing traffic, thus to allocate certain amount of resource execute appropriate policing, classification or scheduling. The core routers in the backbone will do the same checking before executing treatments in order to ensure service-level consistency throughout the whole QoS-enabled network.

AF class 2 (medium drop)	SLA		SLA	
Private Network		DS domain 1		DS domain 2

However, each node may take different attitude toward packets with high priority marking since it may bind with the business deal of SLA among different DS domain owners. It's not easy to achieve deterministic and consistent high-priority QoS traffic throughout the whole network with merely Vigor router's effort.

In the Bandwidth Management menu, click Quality of Service to open the web page.

Status	Bandwidth	Directon	Class 1	Class 2	Class 3	Others	UDP Bandwidth Control	
Enable	10000Kbps/10000Kbps	Outbound	25%	25%	25%	25%	Inactive	Setu
Place Dr	do							
Class Ru Inde		Name				Ru	le Service	Type
	ĸ	Name				Ru <u>Ec</u>		Туре
Inde	к 1	Name					lit	

Bandwidth Management >> Quality of Service

This page displays the QoS settings result of the WAN interface. Click the **Setup** link to access into next page for the general setup of WAN interface. As to class rule, simply click the **Edit** link to access into next for configuration.

You can configure general setup for the WAN interface, edit the Class Rule, and edit the Service Type for the Class Rule for your request.



General Setup for WAN Interface

When you click **Setup**, you can configure the bandwidth ratio for QoS of the WAN interface. There are four queues allowed for QoS control. The first three (Class 1 to Class 3) class rules can be adjusted for your necessity. Yet, the last one is reserved for the packets which are not suitable for the user-defined class rules.

Bandwidth Management >> Q	uality of Service			
General Setup				
Enable the QoS Control	UT 🔽			
WAN Inbound Bar	ndwidth	10000 K	bps	
WAN Outbound B	andwidth	10000 K	bps	
Index C Class 1	lass Name	Reser	ved_band 25	dwidth Ratio %
Class 2			25	96
Class 3			25	%
	Others		25	%
Enable UDP Bandwidth Contro Outbound TCP ACK Prioritize	1	Limite	ed_bandwic	dth Ratio 25 % Online Statistics
(OK Clear	Cancel		
Enable the QoS Control WAN Inbound Bandwidth WAN Outbound Bandwidtl	For example, if your	hich traffic the ng traffic on ing traffic on h incoming click OK , the Statistics line he connection ADSL supp se set 10001 he connection	the QoS (ly. only. and outg and outg nen click (hk appear ng rate of ports 1M kbps for t ng rate of ports 1M	Control settings will going traffic. Setup link again. Y ring on this page. f data input for WA of downstream and this box. The defaul f data output for WA of downstream and
	256K upstream, plea value is 10000kbps.	se set 256kl	bps for th	ns box. The default
Note: The rate of outbound/i correct calculation of QoS. It as 80% - 85% of physical ner performance.	t is suggested to set the	e bandwidth	n value fo	or inbound/outbound
Reserved Bandwidth Ratio	It is reserved for the reserved bandwidth bandwidth to down	n to upstrea	am speed	
Enable UDP Bandwidth Control	Check this and set th field. This is a protec UDP application traf	ction of TCI	P application	tion traffic since



	lots of bandwidth.	lots of bandwidth.								
Outbound TCP ACK Prioritize	The difference in bandwidth between download and upload are great in ADSL2+ environment. For the download speed might be impacted by the uploading TCP ACK, you can check this box to push ACK of upload faster to speed the network traffic.									
Limited_bandwidth Ratio	The ratio typed here is reserved for limited bandwidth of UDP application.									
Online Statistics	Display an online star reference. Bandwidth Management >> Qualit		ty of service for your							
	Online Statistics	Refresh Interva	al: 5 v seconds							
	Index Direction Class Name Rese 1 OUT	25%	0							
	2 OUT	25%	0							
	3 OUT 4 OUT Others	25% 25%	0							
		und Status	10 (8pg)							

Edit the Class Rule for QoS

The first three (Class 1 to Class 3) class rules can be adjusted for your necessity. To add, edit or delete the class rule, please click the **Edit** link of that one.

```
Bandwidth Management >> Quality of Service
```

General Setup Set to Factory Default								
Status	Bandwidth	Directon	Class 1	Class 2	Class 3	Others	UDP Bandwidth Control	
Enable	10000Kbps/10000Kbps	Outbound	25%	25%	25%	25%	Inactive	Setup
Class Rule Index Name Rule								
	,	Namo				Pu	lo Sorvico	Tuno
Inde		Name						Туре
	1	Name				Ru <u>Ec</u>	lit	

After you click the **Edit** link, you will see the following page. Now you can define the name for that Class. In this case, "Test" is used as the name of Class Index #1.



Bandwidth Management >> Quality of Service

Class I	ndex #1							
Name	Test							
NO	Status	Local Address	Remote Address	DiffServ CodePoint	Service Type			
1	Empty	-	-	-	-			
	Add Edit Delete							
			OK Cancel					

For adding a new rule, click **Add** to open the following page.

Bandwidth Management >> Quality of Service

🗹 ACT		
Local Address	Any	Edit
Remote Address	Any	Edit
DiffServ CodePoint	ANY	~
Service Type	ANY	*
Note: Please choose/	setup the <u>Service Typ</u>	<u>e</u> first.

Cancel

OK

ACT	Check this box to invoke these settings.						
Local Address	Click the Edit button to set the local IP address (on LAN) for the rule.						
Remote Address	Click the Edit button to set the remote IP address (on LAN/WAN) for the rule.						
Edit	It allows you to edit source address information.						
🗿 http://192.168.1.1/doc/QosIpEdt.htm - Microsoft Internet Explorer							
	Address Type Subnet Address 💌						
	Start IP Address 0.0.0.0						
	End IP Address						
	Subnet Mask 0.0.0.0						
	OK Close						
	Address Type – Determine the address type for the source						
	address.						
	For Single Address, you have to fill in Start IP address.						
	For Range Address, you have to fill in Start IP address and						
	End IP address.						
	For Subnet Address , you have to fill in Start IP address and Subnet Mask.						
DiffServ CodePoint	All the packets of data will be divided with different levels and will be processed according to the level type by the system.						



	Please assign one of the levels of the data for processing with QoS control.
Service Type	It determines the service type of the data for processing with QoS control. It can also be edited. You can choose the predefined service type from the Service Type drop down list. Those types are predefined in factory. Simply choose the one that you want for using by current QoS.

By the way, you can set up to 20 rules for one Class. If you want to edit an existed rule, please select the radio button of that one and click **Edit** to open the rule edit page for modification.

Class I	ndex #1						
Name	Test						
NO	Status	Local Address	Remote Address	DiffServ CodePoint	Service Type		
1 💿	Active	Any	Any	IP precedence 2	TFTP(UDP:69)		
	Add Edit Delete						
			OK Cancel				

Edit the Service Type for Class Rule

Bandwidth Management >> Quality of Service

To add a new service type, edit or delete an existed service type, please click the Edit link under Service Type field.

```
Bandwidth Management >> Quality of Service
```

General Setup Set to Factory Default							efault	
Status Bandwidth		Directon	Class 1	Class 2	Class 3	Others	UDP Bandwidth Control	
Enable	10000Kbps/10000Kbps	Outbound	25%	25%	25%	25%	Inactive	<u>Setup</u>

Class Rule

Index	Name	Rule	Service Type
Class 1		<u>Edit</u>	
Class 2		<u>Edit</u>	Edit
Class 3		<u>Edit</u>	

After you click the **Edit** link, you will see the following page.

Bandwidth Management >> Quality of Service

User Defined Service Type				
NO	Name	Protocol	Port	
1	Empty	-	-	
Add Edit Delete				
Cancel				

For adding a new service type, click **Add** to open the following page.

Service Type Edit		
Service Na	me	
Service Type Port Configuration		TCP 🖌 6
Туре		💿 Single 🔘 Range
Port Number		0 - 0
Service Name	Type in	a new service for your request.
Service Type	Choose	the type (TCP, UDP or TCP/UDP) for the new service.
have numb Port		ingle or Range as the Type . If you select Range, you type in the starting port number and the end porting on the boxes below. umber – Type in the starting port number and the end number here if you choose Range as the type.

By the way, you can set up to 40 service types. If you want to edit/delete an existed service type, please select the radio button of that one and click **Edit/Edit** for modification.

4.9 Applications

Below shows the menu items for Applications.

Applications
 Dynamic DNS
 Schedule
* RADIUS
 Wake on LAN

4.9.1 Dynamic DNS

The ISP often provides you with a dynamic IP address when you connect to the Internet via your ISP. It means that the public IP address assigned to your router changes each time you access the Internet. The Dynamic DNS feature lets you assign a domain name to a dynamic WAN IP address. It allows the router to update its online WAN IP address mappings on the specified Dynamic DNS server. Once the router is online, you will be able to use the registered domain name to access the router or internal virtual servers from the Internet. It is particularly helpful if you host a web server, FTP server, or other server behind the router.

Before you use the Dynamic DNS feature, you have to apply for free DDNS service to the DDNS service providers. The router provides up to three accounts from three different DDNS service providers. Basically, Vigor routers are compatible with the DDNS services supplied by most popular DDNS service providers such as **www.dyndns.org**, **www.no-ip.com**, **www.dtdns.com**, **www.changeip.com**, **www.dynamic- nameserver.com**. You should visit their websites to register your own domain name for the router.

Enable the Function and Add a Dynamic DNS Account

- 5. Assume you have a registered domain name from the DDNS provider, say *hostname.dyndns.org*, and an account with username: *test* and password: *test*.
- 6. In the DDNS setup menu, check Enable Dynamic DNS Setup.

Dynamic DNS Setup		Set to Factory Default
🗹 Enable Dynamic DN	S Setup (View Log Force Update
Auto-Update interval	1440 Min(s)	
Accounts:		
Index	Domain Name	Active
<u>1.</u>		×
<u>2.</u>		×
<u>3.</u>		×
	OK Clear All	

Applications >> Dynamic DNS Setup

Set to Factory Default Clear all profiles and recover to factory settings.

Enable Dynamic DNS Setup Check this box to enable DDNS function.

Auto-Update IntervalType the time interval for auto update information about
dynamic DNS server.



Index	Click the number below Index to access into the setting page of DDNS setup to set account(s).	
Domain Name	Display the domain name that you set on the setting page of DDNS setup.	
Active	Display if this account is active or inactive.	
View Log	Display DDNS log status.	
Force Update	Force the router updates its information to DDNS server.	

7. Select Index number 1 to add an account for the router. Check **Enable Dynamic DNS Account**, and choose correct Service Provider: dyndns.org, type the registered hostname: *hostname* and domain name suffix: dyndns.org in the **Domain Name** block. The following two blocks should be typed your account Login Name: *test* and Password: *test*.

Applications >> Dynamic DNS Setup >> Dynamic DNS Account Setup

Enable Dynamic DNS	S Account	
Service Provider	dyndns.org (www.dyndns.org)	~
Service Type	Dynamic 🔽	
Domain Name	chronic6683 dyndns.org	dyndns.org 🛩
Login Name	chronic6683	(max. 64 characters)
Password	•••••	(max. 23 characters)
🔲 Wildcards		
🔲 Backup MX		
Mail Extender		

Enable Dynamic DNS Account	Check this box to enable the current account. If you did check the box, you will see a check mark appeared on the Active column of the previous web page in step 2).	
WAN Interface	Select the WAN interface order to apply settings here.	
Service Provider	Select the service provider for the DDNS account.	
Service Type	Select a service type (Dynamic, Custom or Static). If you choose Custom, you can modify the domain that is chosen in the Domain Name field.	
Domain Name	Type in one domain name that you applied previously. Use the drop down list to choose the desired domain.	
Login Name	Type in the login name that you set for applying domain.	
Password	Type in the password that you set for applying domain.	
Click OK how a second description. Yes will be second to have been a		

8. Click **OK** button to activate the settings. You will see your setting has been saved.

The Wildcard and Backup MX features are not supported for all Dynamic DNS providers. You could get more detailed information from their websites.

Disable the Function and Clear all Dynamic DNS Accounts

In the DDNS setup menu, uncheck **Enable Dynamic DNS Setup**, and push **Clear All** button to disable the function and clear all accounts from the router.

Delete a Dynamic DNS Account



In the DDNS setup menu, click the **Index** number you want to delete and then push **Clear All** button to delete the account.

4.9.2 Schedule

The Vigor router has a built-in real time clock which can update itself manually or automatically by means of Network Time Protocols (NTP). As a result, you can not only schedule the router to dialup to the Internet at a specified time, but also restrict Internet access to certain hours so that users can connect to the Internet only during certain hours, say, business hours. The schedule is also applicable to other functions.

You have to set your time before set schedule. In **System Maintenance>> Time and Date** menu, press **Inquire Time** button to set the Vigor router's clock to current time of your PC. The clock will reset once if you power down or reset the router. There is another way to set up time. You can inquiry an NTP server (a time server) on the Internet to synchronize the router's clock. This method can only be applied when the WAN connection has been built up.

Schedule:			Set to Factory Default
Index	Status	Index	Status
<u>1.</u>	х	<u>9.</u>	×
<u>2.</u>	х	<u>10.</u>	×
<u>3.</u>	х	<u>11.</u>	×
<u>4.</u>	х	<u>12.</u>	×
<u>5.</u>	х	<u>13.</u>	×
<u>6.</u>	х	<u>14.</u>	×
<u>7.</u>	х	<u>15.</u>	×
<u>8.</u>	×		

Applications >> Schedule

Status: v --- Active, x --- Inactive

Set to Factory Default	Clear all profiles and recover to factory settings.	
Index	Click the number below Index to access into the setting page of schedule.	
Status	Display if this schedule setting is active or inactive.	

You can set up to 15 schedules. Then you can apply them to your **Internet Access** or **VPN** and **Remote Access** >> **LAN-to-LAN** settings.

To add a schedule, please click any index, say Index No. 1. The detailed settings of the call schedule with index 1 are shown below.

Applications >> Schedule

Index No. 1	
🗹 Enable Schedule Setup	
Start Date (yyyy-mm-dd)	2000 🗸 - 1 🖌 - 1 🖌
Start Time (hh:mm)	0 💙 : 0 💙
Duration Time (hh:mm)	0 💌 : 0 💌
Action	Force On
Idle Timeout	minute(s).(max. 255, 0 for default)
How Often	
Once	
💿 Weekdays	
🗌 Sun 🗹 Mon 🔽	Tue 🗹 Wed 🗹 Thu 🗹 Fri 🔲 Sat
ОК	Clear Cancel

Enable Schedule Setup	Check to enable the schedule.
Start Date (yyyy-mm-dd)	Specify the starting date of the schedule.
Start Time (hh:mm)	Specify the starting time of the schedule.
Duration Time (hh:mm)	Specify the duration (or period) for the schedule.
Action	 Specify which action Call Schedule should apply during the period of the schedule. Force On -Force the connection to be always on. Force Down -Force the connection to be always down. Enable Dial-On-Demand -Specify the connection to be dial-on-demand and the value of idle timeout should be specified in Idle Timeout field. Disable Dial-On-Demand -Specify the connection to be up when it has traffic on the line. Once there is no traffic over idle timeout, the connection will be down and never up again during the schedule.
Idle Timeout	Specify the duration (or period) for the schedule. How often - Specify how often the schedule will be applied Once - The schedule will be applied just once Weekdays - Specify which days in one week should perform the schedule.

Example

Suppose you want to control the PPPoE Internet access connection to be always on (Force On) from 9:00 to 18:00 for whole week. Other time the Internet access connection should be disconnected (Force Down).



1. Make sure the PPPoE connection and **Time Setup** is working properly.



- 2. Configure the PPPoE always on from 9:00 to 18:00 for whole week.
- 3. Configure the **Force Down** from 18:00 to next day 9:00 for whole week.
- 4. Assign these two profiles to the PPPoE Internet access profile. Now, the PPPoE Internet connection will follow the schedule order to perform **Force On** or **Force Down** action according to the time plan that has been pre-defined in the schedule profiles.

4.9.3 RADIUS

Remote Authentication Dial-In User Service (RADIUS) is a security authentication client/server protocol that supports authentication, authorization and accounting, which is widely used by Internet service providers. It is the most common method of authenticating and authorizing dial-up and tunneled network users.

The built-in RADIUS client feature enables the router to assist the remote dial-in user or a wireless station and the RADIUS server in performing mutual authentication. It enables centralized remote access authentication for network management.

Applications >> RADIUS			
RADIUS Setup			
🗹 Enable			
Server IP A	ddress		
Destination	ı Port	1812	
Shared Sec	cret		
Confirm Shared Secret			
Enable	OK Check to	Clear Cancel	.
			-
Server IP Address	Enter the	e IP address of RADIUS server	•
Destination Port		P port number that the RADIU value is 1812, based on RFC 21	•
Shared Secret	authentic	DIUS server and client share a cate the messages sent between gured to use the same shared se	them. Both sides must
Confirm Shared Secret	Re-type	the Shared Secret for confirma	tion.



4.9.4 UPnP

The **UPnP** (Universal Plug and Play) protocol is supported to bring to network connected devices the ease of installation and configuration which is already available for directly connected PC peripherals with the existing Windows 'Plug and Play' system. For NAT routers, the major feature of UPnP on the router is "NAT Traversal". This enables applications inside the firewall to automatically open the ports that they need to pass through a router. It is more reliable than requiring a router to work out by itself which ports need to be opened. Further, the user does not have to manually set up port mappings or a DMZ. **UPnP is available on Windows XP** and the router provide the associated support for MSN Messenger to allow full use of the voice, video and messaging features.

Applications >> UPnP

UPnP
Enable UPnP Service
Enable Connection control Service
Enable Connection Status Service
Enable Connection Status Service

Note: If you intend running UPnP service inside your LAN, you should check the appropriate service above to allow control, as well as the appropriate UPnP settings.

OK	Clear	Cancel

Enable UPNP Service

Accordingly, you can enable either the **Connection Control Service** or **Connection Status Service**.

After setting **Enable UPNP Service** setting, an icon of **IP Broadband Connection on Router** on Windows XP/Network Connections will appear. The connection status and control status will be able to be activated. The NAT Traversal of UPnP enables the multimedia features of your applications to operate. This has to manually set up port mappings or use other similar methods. The screenshots below show examples of this facility.

ress 🔕 Network Connections		😨 IP Broadband Connection on Ro	uter Status ?
Network Tasks	Broadband		
Network Tasks Image: Second system Image: Create a new connection Image: Second system Image: Second system	hinet Disconnected WAN Miniport (PPPOE)	General	Connected
See Also		Duration:	00:19:06
Network Troubleshooter Other Places	test Disconnected DrayTek ISDN PPP	Speed: Activity Internet Internet Gateway	100.0 Mbps My Computer
Control Panel My Network Places My Documents My Computer	IP Broadband Connection on Router Enabled	Packets: Sent: 404 Received: 1,115	734 666
Details 🔹	LAN or High-Speed Internet	Properties Disable	

The UPnP facility on the router enables UPnP aware applications such as MSN Messenger to discover what are behind a NAT router. The application will also learn the external IP address and configure port mappings on the router. Subsequently, such a facility forwards packets from the external ports of the router to the internal ports used by the application.



ieneral	Services
Connect to the Internet using:	Select the services running on your network that Internet users can access.
1P Broadband Connection on Router	Services
This connection allows you to connect to the Internet through a shared connection on another computer.	 □ Ftp Example ♥ msnmsgr (192.168.29.11:13135) 60654 UDP ♥ msnmsgr (192.168.29.11:7824) 13251 UDP ♥ msnmsgr (192.168.29.11:8789) 63231 TCP

The reminder as regards concern about Firewall and UPnP

Can't work with Firewall Software

Enabling firewall applications on your PC may cause the UPnP function not working properly. This is because these applications will block the accessing ability of some network ports.

Security Considerations

Activating the UPnP function on your network may incur some security threats. You should consider carefully these risks before activating the UPnP function.

- Some Microsoft operating systems have found out the UPnP weaknesses and hence you need to ensure that you have applied the latest service packs and patches.
- Non-privileged users can control some router functions, including removing and adding port mappings.

The UPnP function dynamically adds port mappings on behalf of some UPnP-aware applications. When the applications terminate abnormally, these mappings may not be removed.

4.9.5 IGMP

IGMP is the abbreviation of *Internet Group Management Protocol*. It is a communication protocol which is mainly used for managing the membership of Internet Protocol multicast groups.

Applications	>> IGMP					
IGMP						
will access a Enable IGM Enable IGMP	is to act as any multicast IP Snooping 9 Snooping, n	WAN1 a multicast proxy f t group. But this fu nulticast traffic is nulticast traffic is	unction take no only forwarded	o <mark>affect when</mark> to ports that h	Bridge Mode i	s enabled. of that group.
		C)K Can	cel		
Working Multic	ast Groups					<u>Refresh</u>
Index	G	roup ID	P1	P2	P3	P4

Enable IGMP Proxy	Check this box to enable this function. The application of multicast will be executed through WAN or PVC port. In addition, such function is available in NAT mode. WAN1 WAN1 WAN2 PVC
Enable IGMP Snooping	Check this box to enable this function. Multicast traffic will be forwarded to ports that have members of that group. Disabling IGMP snooping will make multicast traffic treated in the same manner as broadcast traffic.
Group ID	This field displays the ID port for the multicast group. The available range for IGMP starts from 224.0.0.0 to 239.255.255.254.
P1 to P4	It indicates the LAN port used for the multicast group.
Refresh Click this link to	renew the working multicast group status.

If you check Enable IGMP Proxy, you will get the following page. All the multicast groups will be listed and all the LAN ports (P1 to P4) are available for use.

4.9.6 Wake on LAN

A PC client on LAN can be woken up by the router it connects. When a user wants to wake up a specified PC through the router, he/she must type correct MAC address of the specified PC on this web page of **Wake on LAN** of this router.

In addition, such PC must have installed a network card supporting WOL function. By the way, WOL function must be set as "Enable" on the BIOS setting.



Application >> Wake on LAN

Wake on LAN

Wake by:	MAC Address 🗸	
IP Address:	🕅	
MAC Address:	Wake Up!	
Result		

Wake by

Two types provide for you to wake up the binded IP. If you choose Wake by MAC Address, you have to type the correct MAC address of the host in MAC Address boxes. If you choose Wake by IP Address, you have to choose the correct IP address.

_

	Wake by:	MAC Address 🚩
		MAC Address
		IP Address
IP Address	IP to MAC will b	that have been configured in Firewall>>Bind be shown in this drop down list. Choose the IP drop down list that you want to wake up.
MAC Address	Type any one of t	he MAC address of the bound PCs.
Wake Up		to wake up the selected IP. See the following will be shown on the box.

Application >> Wake on LAN

IP Address: V MAC Address: ::::::::::::::::::::::::::::::::::	Note: Wake on can wake up thr	LAN integrates with <u>Bind IP to MAC</u> function, only binded PCs ough IP.
MAC Address:	Wake by:	MAC Address 💌
	IP Address:	😒
Posult	MAC Address:	Wake Up!
Result	Result	

4.10 VPN and Remote Access

A Virtual Private Network (VPN) is the extension of a private network that encompasses links across shared or public networks like the Internet. In short, by VPN technology, you can send data between two computers across a shared or public network in a manner that emulates the properties of a point-to-point private link.

Below shows the menu items for VPN and Remote Access.

VPN and Remote Access
Remote Dial-in User
= LAN to LAN

4.10.1 Remote Access Control

Enable the necessary VPN service as you need. If you intend to run a VPN server inside your LAN, you should disable the VPN service of Vigor Router to allow VPN tunnel pass through, as well as the appropriate NAT settings, such as DMZ or open port.

VPN and Remote Access >> Remote Access Control Setup

Remote Access Control Setup	
	Enable PPTP VPN Service
	Enable IPSec VPN Service
	Enable L2TP VPN Service

Note: If you intend running a VPN server inside your LAN, you should uncheck the appropriate protocol above to allow pass-through, as well as the appropriate NAT settings.



4.10.2 PPP General Setup

This submenu only applies to PPP-related VPN connections, such as PPTP, L2TP, L2TP over IPSec.

VPN and Remote Access >> PPP	General Setu	qı	
PPP General Setup			
PPP/MP Protocol		IP Address Assignmer	
Dial-In PPP Authentication PAP or CHAP	*	(When DHCP Disable s Start IP Address	et) 192.168.1.200
Dial-In PPP Encryption (MPPE) Optional MPPI	E 💌		L
Mutual Authentication (PAP) 🛛 🔘 Y	es 📀 No		
Username			
Password			
)K	



Dial-In PPP Authentication PAP Only	Select this option to force the router to authenticate dial-in users with the PAP protocol.
PAP or CHAP	Selecting this option means the router will attempt to authenticate dial-in users with the CHAP protocol first. If the dial-in user does not support this protocol, it will fall back to use the PAP protocol for authentication.
Dial-In PPP Encryption (MPPE Optional MPPE	This option represents that the MPPE encryption method will be optionally employed in the router for the remote dial-in user. If the remote dial-in user does not support the MPPE encryption algorithm, the router will transmit "no MPPE encrypted packets". Otherwise, the MPPE encryption scheme will be used to encrypt the data. Optional MPPE Pequire MPPE(40/128 bit) Maximum MPPE(128 bit) Maximum MPPE(128 bit) Selecting this option will force the router to encrypt packets by using the MPPE encryption algorithm. In addition, the remote dial-in user will use 40-bit to perform encryption prior to using 128-bit for encryption. In other words, if 128-bit MPPE encryption method is not available, then 40-bit encryption scheme will be applied to encrypt the data. Maximum MPPE - This option indicates that the router will use the MPPE encryption scheme with maximum bits (128-bit) to encrypt the data.
Mutual Authentication (PAP)	The Mutual Authentication function is mainly used to communicate with other routers or clients who need bi-directional authentication in order to provide stronger security, for example, Cisco routers. So you should enable this function when your peer router requires mutual authentication. You should further specify the User Name and Password of the mutual authentication peer.
Start IP Address	Enter a start IP address for the dial-in PPP connection. You should choose an IP address from the local private network. For example, if the local private network is 192.168.1.0/255.255.255.0, you could choose 192.168.1.200 as the Start IP Address.

4.10.3 IPSec General Setup

In IPSec General Setup, there are two major parts of configuration.

There are two phases of IPSec.

- Phase 1: negotiation of IKE parameters including encryption, hash, Diffie-Hellman parameter values, and lifetime to protect the following IKE exchange, authentication of both peers using either a Pre-Shared Key or Digital Signature (x.509). The peer that starts the negotiation proposes all its policies to the remote peer and then remote peer tries to find a highest-priority match with its policies. Eventually to set up a secure tunnel for IKE Phase 2.
- Phase 2: negotiation IPSec security methods including Authentication Header (AH) or Encapsulating Security Payload (ESP) for the following IKE exchange and mutual examination of the secure tunnel establishment.



There are two encapsulation methods used in IPSec, **Transport** and **Tunnel**. The **Transport** mode will add the AH/ESP payload and use original IP header to encapsulate the data payload only. It can just apply to local packet, e.g., L2TP over IPSec. The **Tunnel** mode will not only add the AH/ESP payload but also use a new IP header (Tunneled IP header) to encapsulate the whole original IP packet.

Authentication Header (AH) provides data authentication and integrity for IP packets passed between VPN peers. This is achieved by a keyed one-way hash function to the packet to create a message digest. This digest will be put in the AH and transmitted along with packets. On the receiving side, the peer will perform the same one-way hash on the packet and compare the value with the one in the AH it receives.

Encapsulating Security Payload (ESP) is a security protocol that provides data confidentiality and protection with optional authentication and replay detection service.

VPN and Remote Access >> IPSec Gene	eral Setup
VPN IKE/IPSec General Setup	
Dial-in Set up for Remote Dial-in users and D	ynamic IP Client (LAN to LAN).
IKE Authentication Method	
Pre-Shared Key	
Confirm Pre-Shared Key	
IPSec Security Method	
Medium (AH)	
Data will be authentic, but will no	t be encrypted.
High (ESP) 🔽 DES 🔽 3DES	V AES
Data will be encrypted and authe	ntic.



IKE Authentication Method This usually applies to those are remote dial-in user or node (LAN-to-LAN) which uses dynamic IP address and IPSec-related VPN connections such as L2TP over IPSec and IPSec tunnel. Pre-Shared Key -Currently only support Pre-Shared Key authentication. Pre-Shared Key- Specify a key for IKE authentication **Confirm Pre-Shared Key-** Retype the characters to confirm the pre-shared key. **IPSec Security Method** Medium - Authentication Header (AH) means data will be authenticated, but not be encrypted. By default, this option is active. High - Encapsulating Security Payload (ESP) means payload (data) will be encrypted and authenticated. You may select encryption algorithm from Data Encryption Standard (DES), Triple DES (3DES), and AES.

.10.4 IPSec Peer Identity

To use digital certificate for peer authentication in either LAN-to-LAN connection or Remote User Dial-In connection, here you may edit a table of peer certificate for selection. As shown below, the router provides **32** entries of digital certificates for peer dial-in users.

Index	Name	Status	Index	Name	Status
<u>1.</u>	???	×	<u>17.</u>	???	Х
<u>2.</u>	???	×	<u>18.</u>	???	X
<u>3.</u>	???	×	<u>19.</u>	???	X
<u>4.</u>	???	×	<u>20.</u>	???	X
<u>5.</u>	???	×	<u>21.</u>	???	X
<u>6.</u>	???	×	<u>22.</u>	???	X
<u>7.</u>	???	×	<u>23.</u>	???	Х
<u>8.</u>	???	×	<u>24.</u>	???	×
<u>9.</u>	???	×	<u>25.</u>	???	Х
<u>10.</u>	???	×	<u>26.</u>	???	X
<u>11.</u>	???	×	<u>27.</u>	???	×
<u>12.</u>	???	×	<u>28.</u>	???	X
<u>13.</u>	???	×	<u>29.</u>	???	×
<u>14.</u>	???	×	<u>30.</u>	???	×
<u>15.</u>	???	×	<u>31.</u>	???	×
<u>16.</u>	???	×	<u>32.</u>	???	X



Set to Factory Default	Click it to clear all indexes.
Index	Click the number below Index to access in

Click the number below Index to access into the setting page of IPSec Peer Identity.

Name

Display the profile name of that index.

Click each index to edit one peer digital certificate. There are three security levels of digital signature authentication: Fill each necessary field to authenticate the remote peer. The following explanation will guide you to fill all the necessary fields.

VPN and Remote Access >> IPSec Peer Identity

Profile Index : 1	
Profile Name ???	
☑Enable this account	
Accept Any Peer ID	
O Accept Subject Alternative Na	ame
Туре	IP Address 🛛 🔽
IP	
O Accept Subject Name	
Country (C)	
State (ST)	
Location (L)	
Orginization (O)	
Orginization Unit (OU)	
Common Name (CN)	
Email (E)	
	OK Clear Cancel
Profile Name	Type in .
Accept Any Peer ID	Click to accept any peer regardless of its identity.
Accept Subject Alternative Name	Click to check one specific field of digital signature to accept the peer with matching value. The field can be IP Address , Domain , or E-mail Address . The box under the Type will appear according to the type you select and ask you to fill in corresponding setting.
Accept Subject Name	Click to check the specific fields of digital signature to accept the peer with matching value. The field includes Country (C), State (ST), Location (L), Organization (O), Organization Unit (OU), Common Name (CN), and Email (E).

4.10.5 Remote Dial-in User

You can manage remote access by maintaining a table of remote user profile, so that users can be authenticated to dial-in via VPN connection. You may set parameters including specified connection peer ID, connection type (VPN connection - including PPTP, IPSec Tunnel, and L2TP by itself or over IPSec) and corresponding security methods, etc.

The router provides **32** access accounts for dial-in users. Besides, you can extend the user accounts to the RADIUS server through the built-in RADIUS client function. The following figure shows the summary table.

Index	User	Status	Index	User	Status
<u>1.</u>	???	×	<u>17.</u>	???	×
<u>2.</u>	???	×	<u>18.</u>	???	×
<u>3.</u>	???	×	<u>19.</u>	???	X
<u>4.</u>	???	×	<u>20.</u>	???	X
<u>5.</u>	???	×	<u>21.</u>	???	X
<u>6.</u>	???	×	<u>22.</u>	???	X
<u>7.</u>	???	×	<u>23.</u>	???	Х
<u>8.</u>	???	×	<u>24.</u>	???	×
<u>9.</u>	???	×	<u>25.</u>	???	×
<u>10.</u>	???	×	<u>26.</u>	???	×
<u>11.</u>	???	×	<u>27.</u>	???	×
<u>12.</u>	???	×	<u>28.</u>	???	×
<u>13.</u>	???	×	<u>29.</u>	???	×
<u>14.</u>	???	×	<u>30.</u>	???	×
<u>15.</u>	???	×	<u>31.</u>	???	X
<u>16.</u>	???	×	<u>32.</u>	???	X

VPN and Remote Access >> Remote Dial-in User

Set to Factory Default	Click to clear all indexes.
Index	Click the number below Index to access into the setting page of Remote Dial-in User.
User	Display the username for the specific dial-in user of the LAN-to-LAN profile. The symbol ??? represents that the profile is empty.
Status	Display the access state of the specific dial-in user. The symbol V and X represent the specific dial-in user to be active and inactive, respectively.

Click each index to edit one remote user profile. **Each Dial-In Type requires you to fill the different corresponding fields on the right.** If the fields gray out, it means you may leave it untouched. The following explanation will guide you to fill all the necessary fields.

VPN and Remote Access >> Remote Dial-in User

Index No. 1	
User account and Authentication	Username ???
Enable this account	Password
Idle Timeout 300 second(s)	
	IKE Authentication Method
Allowed Dial-In Type	🛛 🗹 Pre-Shared Key
🗹 РРТР	IKE Pre-Shared Key
🗹 IPSec Tunnel	Digital Signature(X.509)
☑ L2TP with IPSec Policy None	None V
Specify Remote Node	
Remote Client IP or Peer ISDN Number	IPSec Security Method
	Medium(AH)
	High(ESP) 🗹 DES 🗹 3DES 🗹 AES
or Peer ID	Local ID (optional)
Netbios Naming Packet 💿 Pass 🔘 Block	

Enable this account	Check the box to enable this function. Idle Timeout- If the dial-in user is idle over the limitation of the timer, the router will drop this connection. By default, the Idle Timeout is set to 300 seconds.
РРТР	Allow the remote dial-in user to make a PPTP VPN connection through the Internet. You should set the User Name and Password of remote dial-in user below
IPSec Tunnel	Allow the remote dial-in user to make an IPSec VPN connection through Internet.
L2TP	 Allow the remote dial-in user to make a L2TP VPN connection through the Internet. You can select to use L2TP alone or with IPSec. Select from below: None - Do not apply the IPSec policy. Accordingly, the VPN connection employed the L2TP without IPSec policy can be viewed as one pure L2TP connection. Nice to Have - Apply the IPSec policy first, if it is applicable during negotiation. Otherwise, the dial-in VPN connection becomes one pure L2TP connection. Must -Specify the IPSec policy to be definitely applied on the L2TP connection.
Specify Remote Node	 Check the checkbox-You can specify the IP address of the remote dial-in user, ISDN number or peer ID (used in IKE aggressive mode). Uncheck the checkbox-This means the connection type you select above will apply the authentication methods and security methods in the general settings.
Netbios Naming Packet	Pass – Click it to have an inquiry for data transmission between the hosts located on both sides of VPN Tunnel while connecting. Block – When there is conflict occurred between the hosts on both sides of VPN Tunnel in connecting, such function can

	block data transmission of Netbios Naming Packet inside the tunnel.
User Name	This field is applicable when you select PPTP or L2TP with or without IPSec policy above.
Password	This field is applicable when you select PPTP or L2TP with or without IPSec policy above.
IKE Authentication Method	 d This group of fields is applicable for IPSec Tunnels and L2TP with IPSec Policy when you specify the IP address of the remote node. The only exception is Digital Signature (X.509) can be set when you select IPSec tunnel either with or without specify the IP address of the remote node. Pre-Shared Key - Check the box of Pre-Shared Key to invoke this function and type in the required characters (1-63) as the pre-shared key. Digital Signature (X.509) – Check the box of Digital Signature to invoke this function and Select one predefined Profiles set in the VPN and Remote Access >>IPSec Peer Identity.
IPSec Security Method	This group of fields is a must for IPSec Tunnels and L2TP with IPSec Policy when you specify the remote node. Check the Medium, DES, 3DES or AES box as the security method. Medium -Authentication Header (AH) means data will be authenticated, but not be encrypted. By default, this option is invoked. You can uncheck it to disable it. High-Encapsulating Security Payload (ESP) means payload (data) will be encrypted and authenticated. You may select encryption algorithm from Data Encryption Standard (DES), Triple DES (3DES), and AES. Local ID - Specify a local ID to be used for Dial-in setting in the LAN-to-LAN Profile setup. This item is optional and can be used only in IKE aggressive mode.

4.10.6 LAN to LAN

Here you can manage LAN-to-LAN connections by maintaining a table of connection profiles. You may set parameters including specified connection direction (dial-in or dial-out), connection peer ID, connection type (VPN connection - including PPTP, IPSec Tunnel, and L2TP by itself or over IPSec) and corresponding security methods, etc.

The router supports 2 VPN tunnels simultaneously and provides up to **32** profiles. The following figure shows the summary table.

Index	Name	Status	Index	Name	Status
<u>1.</u>	???	X	<u>17.</u>	???	X
<u>2.</u>	???	X	<u>18.</u>	???	×
<u>3.</u>	???	X	<u>19.</u>	???	×
<u>4.</u>	???	X	<u>20.</u>	???	×
<u>5.</u>	???	X	<u>21.</u>	???	×
<u>6.</u>	???	X	<u>22.</u>	???	×
<u>7.</u>	???	×	<u>23.</u>	???	×
<u>8.</u>	???	X	<u>24.</u>	???	×
<u>9.</u>	???	X	<u>25.</u>	???	×
<u>10.</u>	???	X	<u>26.</u>	???	×
<u>11.</u>	???	×	<u>27.</u>	???	×
<u>12.</u>	???	X	<u>28.</u>	???	X
<u>13.</u>	???	X	<u>29.</u>	???	×
<u>14.</u>	???	X	<u>30.</u>	???	×
<u>15.</u>	???	×	<u>31.</u>	???	×
<u>16.</u>	???	×	<u>32.</u>	???	×

VPN and Remote Access >> LAN to LAN

Name

Click to clear all indexes.

Indicate the name of the LAN-to-LAN profile. The symbol **???** represents that the profile is empty.

Status

Indicate the status of individual profiles. The symbol V and X represent the profile to be active and inactive, respectively.

Click each index to edit each profile and you will get the following page. Each LAN-to-LAN profile includes 4 subgroups. If the fields gray out, it means you may leave it untouched. The following explanations will guide you to fill all the necessary fields.

For the web page is too long, we divide the page into several sections for explanation.

VPN and Remote Access >> LAN to LAN

Profile Index : 1

1. Common Settings			
Profile Name Enable this profile Netbios Naming Packet	??? ⊙ Pass ○ Block	Call Direction Both Always on Idle Timeout Enable PING to keep a PING to the IP	O Dial-Out O Dial-In 300 second(s) alive
2. Dial-Out Settings		1	
Type of Server I am call PPTP IPSec Tunnel L2TP with IPSec Polic Server IP/Host Name for V (such as draytek.com or 3	y None	Username Password PPP Authentication VJ Compression IKE Authentication Metl Pre-Shared Key IKE Pre-Shared Key Digital Signature(X.50 None IPSec Security Method Medium(AH) High(ESP) DES without Advanced Index(1-15) in Schedule , , , ,	9)

Profile Name	Specify a name for the profile of the LAN-to-LAN connection.
Enable this profile	Check here to activate this profile.
Netbios Naming Packet	Pass – click it to have an inquiry for data transmission between the hosts located on both sides of VPN Tunnel while connecting. Block – When there is conflict occurred between the hosts on both sides of VPN Tunnel in connecting, such function can block data transmission of Netbios Naming Packet inside the tunnel.
Call Direction	Specify the allowed call direction of this LAN-to-LAN profile. Both :-initiator/responder Dial-Out - initiator only Dial-In- responder only.
Always On or Idle Timeout	Always On-Check to enable router always keep VPN connection.Idle Timeout: The default value is 300 seconds. If the connection has been idled over the value, the router will drop the connection.
Enable PING to keep alive	This function is to help the router to determine the status of IPSec VPN connection, especially useful in the case of abnormal VPN IPSec tunnel disruption. For details, please refer to the note below. Check to enable the transmission of PING packets to a specified IP address.



PING to the IP	Enter the IP address of the remote host that located at the other-end of the VPN tunnel.		
	 Enable PING to Keep Alive is used to handle abnormal IPSec VPN connection disruption. It will help to provide the state of a VPN connection for router's judgment of redial. Normally, if any one of VPN peers wants to disconnect the connection, it should follow a serial of packet exchange procedure to inform each other. However, if the remote peer disconnect without notice, Vigor router will by no where to know this situation. To resolve this dilemma, by continuously sending PING packets to the remote host, the Vigor router can know the true existence of this VPN connection and react accordingly. This is independent of DPD (dead peer detection). 		
РРТР	Build a PPTP VPN connection to the server through the Internet. You should set the identity like User Name and Password below for the authentication of remote server.		
IPSec Tunnel	Build an IPSec VPN connection to the server through Internet.		
L2TP with	 Build a L2TP VPN connection through the Internet. You can select to use L2TP alone or with IPSec. Select from below: None: Do not apply the IPSec policy. Accordingly, the VPN connection employed the L2TP without IPSec policy can be viewed as one pure L2TP connection. Nice to Have: Apply the IPSec policy first, if it is applicable during negotiation. Otherwise, the dial-out VPN connection becomes one pure L2TP connection. Must: Specify the IPSec policy to be definitely applied on the L2TP connection. 		
User Name	This field is applicable when you select, PPTP or L2TP with or without IPSec policy above.		
Password	This field is applicable when you select PPTP or L2TP with or without IPSec policy above.		
PPP Authentication	This field is applicable when you select, PPTP or L2TP with or without IPSec policy above. PAP/CHAP is the most common selection due to wild compatibility.		
VJ compression	This field is applicable when you select PPTP or L2TP with or without IPSec policy above. VJ Compression is used for TCP/IP protocol header compression. Normally set to Yes to improve bandwidth utilization.		
IKE Authentication Method	This group of fields is applicable for IPSec Tunnels and L2TP with IPSec Policy. Pre-Shared Key - Input 1-63 characters as pre-shared key. Digital Signature (X.509) - Select one predefined Profiles set in the VPN and Remote Access >> IPSec Peer Identity .		
IPSec Security Method	This group of fields is a must for IPSec Tunnels and L2TP with IPSec Policy.		
Medium	Authentication Header (AH) means data will be authenticated, but not be encrypted. By default, this option is active.		



High (ESP-Encapsulating Security Payload)- means payload (data) will be encrypted and authenticated. Select from below: **DES without Authentication** -Use DES encryption algorithm and not apply any authentication scheme.

DES with Authentication-Use DES encryption algorithm and apply MD5 or SHA-1 authentication algorithm.

3DES without Authentication-Use triple DES encryption algorithm and not apply any authentication scheme.

3DES with Authentication-Use triple DES encryption algorithm and apply MD5 or SHA-1 authentication algorithm. **AES without Authentication-**Use AES encryption algorithm and not apply any authentication scheme.

AES with Authentication-Use AES encryption algorithm and apply MD5 or SHA-1 authentication algorithm.

Advanced

Specify mode, proposal and key life of each IKE phase, Gateway, etc.

The window of advance setup is shown as below:

IKE phase 1 mode	Main mode	O Aggressive mode
•	-	55
IKE phase 1 proposal		SHA1_G1/3DES_MD5_G1/3DES_MD5_G2 💌
IKE phase 2 proposal	HMAC_SHA1/HMAC	_MD5 💙
IKE phase 1 key lifetime	28800	(900 ~ 86400)
IKE phase 2 key lifetime	3600	(600 ~ 86400)
Perfect Forward Secret	💿 Disable	🔘 Enable
Local ID		

IKE phase 1 mode -Select from **Main** mode and **Aggressive** mode. The ultimate outcome is to exchange security proposals to create a protected secure channel. **Main** mode is more secure than **Aggressive** mode since more exchanges are done in a secure channel to set up the IPSec session. However, the **Aggressive** mode is faster. The default value in Vigor router is Main mode.

IKE phase 1 proposal-To propose the local available authentication schemes and encryption algorithms to the VPN peers, and get its feedback to find a match. Two combinations are available for Aggressive mode and nine for **Main** mode. We suggest you select the combination that covers the most schemes.

IKE phase 2 proposal-To propose the local available algorithms to the VPN peers, and get its feedback to find a match. Three combinations are available for both modes. We suggest you select the combination that covers the most algorithms.

IKE phase 1 key lifetime-For security reason, the lifetime of key should be defined. The default value is 28800 seconds. You may specify a value in between 900 and 86400 seconds. **IKE phase 2 key lifetime-**For security reason, the lifetime of key should be defined. The default value is 3600 seconds. You may specify a value in between 600 and 86400 seconds. **Perfect Forward Secret (PFS)-**The IKE Phase 1 key will be



reused to avoid the computation complexity in phase 2. The default value is inactive this function.

Local ID-In **Aggressive** mode, Local ID is on behalf of the IP address while identity authenticating with remote VPN server. The length of the ID is limited to 47 characters.

3. Dial-In Settings			
Allowed Dial-In Type		_	000
РРТР		Username	???
🗹 IPSec Tunnel		Password	
☑ L2TP with IPSec Po	licy None 🔽	VJ Compression	💿 On 🔘 Off
Specify Remote VPN Peer VPN Server IP or Peer ID		IKE Authentication Met ✓ Pre-Shared Key IKE Pre-Shared Key Digital Signature(X.50) None IPSec Security Method ✓ Medium(AH) High(ESP) ✓ DES ✓	D9)
4. TCP/IP Network Set			
My WAN IP	0.0.0.0	RIP Direction	Disable 👻
Remote Gateway IP	0.0.0.0	do	ote network, you have to
Remote Network IP	0.0.0.0		Route 🛩
Remote Network Mask	255.255.255.0		
	More	Change default route single WAN supports this	to this VPN tunnel (Only)
llowed Dial-In Type PTP	e Determine the Allow the rem through the In	dial-in connection with ote dial-in user to make ternet. You should set t emote dial-in user below	e a PPTP VPN connec he User Name and

iniowed Blai in 19pe	Determine the data in connection with different types.
PPTP	Allow the remote dial-in user to make a PPTP VPN connection through the Internet. You should set the User Name and Password of remote dial-in user below.
IPSec Tunnel	Allow the remote dial-in user to trigger an IPSec VPN connection through Internet.
L2TP	 Allow the remote dial-in user to make a L2TP VPN connection through the Internet. You can select to use L2TP alone or with IPSec. Select from below: None - Do not apply the IPSec policy. Accordingly, the VPN connection employed the L2TP without IPSec policy can be viewed as one pure L2TP connection. Nice to Have - Apply the IPSec policy first, if it is applicable during negotiation. Otherwise, the dial-in VPN connection becomes one pure L2TP connection. Must - Specify the IPSec policy to be definitely applied on the L2TP connection.
Specify Remote VPN Gateway	You can specify the IP address of the remote dial-in user or peer ID (should be the same with the ID setting in dial-in



	type) by checking the box. Also, you should further specify the corresponding security methods on the right side.
	If you uncheck the checkbox, the connection type you select above will apply the authentication methods and security methods in the general settings.
User Name	This field is applicable when you select PPTP or L2TP with or without IPSec policy above.
Password	This field is applicable when you select PPTP or L2TP with or without IPSec policy above.
VJ Compression	VJ Compression is used for TCP/IP protocol header compression. This field is applicable when you select PPTP or L2TP with or without IPSec policy above.
IKE Authentication Method	This group of fields is applicable for IPSec Tunnels and L2TP with IPSec Policy when you specify the IP address of the remote node. The only exception is Digital Signature (X.509) can be set when you select IPSec tunnel either with or without specify the IP address of the remote node. Pre-Shared Key - Check the box of Pre-Shared Key to invoke this function and type in the required characters (1-63) as the pre-shared key. Digital Signature (X.509) –Check the box of Digital Signature to invoke this function and select one predefined Profiles set in the VPN and Remote Access >> IPSec Peer Identity .
IPSec Security Method	This group of fields is a must for IPSec Tunnels and L2TP with
	 IPSec Policy when you specify the remote node. Medium- Authentication Header (AH) means data will be authenticated, but not be encrypted. By default, this option is active. High- Encapsulating Security Payload (ESP) means payload (data) will be encrypted and authenticated. You may select encryption algorithm from Data Encryption Standard (DES), Triple DES (3DES), and AES.
My WAN IP	 Medium- Authentication Header (AH) means data will be authenticated, but not be encrypted. By default, this option is active. High- Encapsulating Security Payload (ESP) means payload (data) will be encrypted and authenticated. You may select
My WAN IP Remote Gateway IP	 Medium- Authentication Header (AH) means data will be authenticated, but not be encrypted. By default, this option is active. High- Encapsulating Security Payload (ESP) means payload (data) will be encrypted and authenticated. You may select encryption algorithm from Data Encryption Standard (DES), Triple DES (3DES), and AES. This field is only applicable when you select PPTP or L2TP with or without IPSec policy above. The default value is 0.0.0, which means the Vigor router will get a PPP IP address from the remote router during the IPCP negotiation phase. If the PPP IP address is fixed by remote side, specify the fixed IP address here. Do not change the default value if you do not select PPTP



	phase 2 quick mode.
More	Add a static route to direct all traffic destined to more Remote Network IP Addresses/ Remote Network Mask through the VPN connection. This is usually used when you find there are several subnets behind the remote VPN router.
RIP Direction	The option specifies the direction of RIP (Routing Information Protocol) packets. You can enable/disable one of direction here. Herein, we provide four options: TX/RX Both, TX Only, RX Only, and Disable.
From first subnet to remote network, you have to do	If the remote network only allows you to dial in with single IP, please choose NAT , otherwise choose Route .
Change default route to this VPN tunnel	Check this box to change the default route with this VPN tunnel.

4.10.7 Connection Management

You can find the summary table of all VPN connections. You may disconnect any VPN connection by clicking **Drop** button. You may also aggressively Dial-out by using Dial-out Tool and clicking **Dial** button.

VPN and	d Remote Ac	cess >> Connec	tion Manager	ment				
Dial-out	Tool				Refre	sh Sec	onds : 10	Refresh
					🗸 Dial]		
VPN Con Current P	nection State age: 1	us				Pa	ige No.	Go >>
VPN	Туре	Remote IP	Virtual Network	Tx Pkts	Tx Rate (Bps)	Rx Pkts	Rx Rate (Bps)	UpTime
1					×××××× : C ×××××× : C			
Dial		Clic	k this button	to exec	cute dial	out fui	nction.	
Refresh	Seconds		Choose the time for refresh the dial information among 5, 10, and 30.					
Refresh	l	Clic	k this button	to refre	esh the w	hole c	onnectio	on status.

4.11 Certificate Management

A digital certificate works as an electronic ID, which is issued by a certification authority (CA). It contains information such as your name, a serial number, expiration dates etc., and the digital signature of the certificate-issuing authority so that a recipient can verify that the certificate is real. Here Vigor router support digital certificates conforming to standard X.509.

Any entity wants to utilize digital certificates should first request a certificate issued by a CA server. It should also retrieve certificates of other trusted CA servers so it can authenticate the peer with certificates issued by those trusted CA servers.

Here you can manage generate and manage the local digital certificates, and set trusted CA certificates. Remember to adjust the time of Vigor router before using the certificate so that you can get the correct valid period of certificate.

Below shows the menu items for Certificate Management.

Certificate Management
Local Certificate
 Certificate Backup

4.11.1 Local Certificate

Certificate Management >> Local Certificate

X509 Local Certificate Configuration



Generate

Click this button to open Generate Certificate Request window.



Subject Alternative Name	
Туре	IP Address
IP	
Subject Name	
Country (C)	
State (ST)	
Location (L)	
Orginization (O)	
Orginization Unit (OU)	
Common Name (CN)	
Email (E)	
Кеу Туре	RSA Y
Key Size	1024 Bit 🗸

Generate

Type in all the information that the window requests. Then click **Generate** again.

Import	Click this button to import a saved file as the certification information.
Refresh	Click this button to refresh the information listed below.
View	Click this button to view the detailed settings for certificate request.

Certificate Management >> Local Certificate

After clicking **Generate**, the generated information will be displayed on the window below:

Certificate Management >> Local Certificate

Name	Subject	Status	Modify
Local	/C=TW/ST=HC/L=HC/O=Draytek/0	Requesting	View Delete
GENERATE	IMPORT REFRESH		
MIIBq EwJIQ: CQEWES AoGBAI a1X//1 m6+0f4 hkiG9u 9yojHp eorpDs	BEGIN CERTIFICATE REQUEST CCARMCAQAwajELMAkGA1UEBhMCVFcxCzAJ EQMA4GA1UEChMHRHJheXR1azELMAkGA1UE N1cHBvcnRA2HJheXR1ay5jb2Owg28wDQYJ MJdTsqfF97FEpYy+IqeJVJGuSRtqG6Etw8 GnEccQ42LPSQIQ85Qychwq07Bm0EDf10wH txZ4QQnjXXgciC0Bj1iAa6MLScelsynZhkg JOBAQUFAAOBgQCq3sdwVc21t9qn4U6X2BJs DstNsmWsMRuAwGeKCWc8S/gLtHhr6iccMoT a1/rC92wCra0t8XUmPqNoiytq8BxStTE8vU ND CERTIFICATE REOUEST	CxMCUkQxIjAg KoZIhvcNAQEB YTUSHQvXpAzc: wCalAZQoGvIi nQ1QNSuFAgMB Vzu7JHafSSeU oQFx/LWdaEPU	BgkqhkiG9w0B BQADgY0AMIGJ rgJBGrikTUBX DDMC7f5w9xA8 AAGgADANBgkq naYDZefCmGfX 5LqryBKKgC9t

X509 Local Certificate Configuration



4.11.2 Trusted CA Certificate

Trusted CA certificate lists three sets of trusted CA certificate.

Certificate Management >> Trusted CA Certificate							
X509 Trusted CA Ce	ertificate Configuration						
Name	Subject	Status	Modify				
Trusted CA-1			View Delete				
Trusted CA-2			View Delete				
Trusted CA-3			View Delete				
	IMPORT RI	EFRESH					

To import a pre-saved trusted CA certificate, please click **IMPORT** to open the following window. Use **Browse...** to find out the saved text file. Then click **Import**. The one you imported will be listed on the Trusted CA Certificate window. Then click **Import** to use the pre-saved file.

Certificate Management >> Trusted CA Certificate

mport X509 Trusted CA Certificate	
Select a trusted CA certificate file.	
Browse.	
Click Import to upload the certification.	
Import Cancel	

For viewing each trusted CA certificate, click **View** to open the certificate detail information window. If you want to delete a CA certificate, choose the one and click **Delete** to remove all the certificate information.

🕘 http	://192.168.1.5 - Certificate Informat	ion - Microsoft Internet Explorer	
			^
	Certific	ate Detail Information	
	Certificate Name:	Trusted CA-1	
	Issuer:		
	Subject:		Ш
	Subject Alternative Name:		
	Valid From:		
	Valid To:		
		Close	~
e			

4.11.3 Certificate Backup

Local certificate and Trusted CA certificate for this router can be saved within one file. Please click **Backup** on the following screen to save them. If you want to set encryption password for these certificates, please type characters in both fields of **Encrypt password** and **Retype password**.

Also, you can use **Restore** to retrieve these two settings to the router whenever you want.

Certificate Ma	Certificate Management >> Certificate Backup				
Certificate Ba	ertificate Backup / Restoration				
Backup					
	Encrypt password:				
	Confirm password:				
	Click Backup to download certificates to your local PC as a file.				
Restoration					
	Select a backup file to restore.				
	Browse				
	Decrypt password:				
	Click Restore to upload the file.				

4.12 VoIP

Voice over IP network (VoIP) enables you to use your broadband Internet connection to make toll quality voice calls over the Internet.

There are many different call signaling protocols, methods by which VoIP devices can talk to each other. The most popular protocols are SIP, MGCP, Megaco and H.323. These protocols are not all compatible with each other (except via a soft-switch server).

The Vigor V models support the SIP protocol as this is an ideal and convenient deployment for the ITSP (Internet Telephony Service Provider) and softphone and is widely supported. SIP is an end-to-end, signaling protocol that establishes user presence and mobility in VoIP structure. Every one who wants to talk using his/her SIP Uniform Resource Identifier, "SIP Address". The standard format of SIP URI is

sip: user:password @ host: port

Some fields may be optional in different use. In general, "host" refers to a domain. The "userinfo" includes the user field, the password field and the @ sign following them. This is very similar to a URL so some may call it "SIP URL". SIP supports peer-to-peer direct calling and also calling via a SIP proxy server (a role similar to the gatekeeper in H.323 networks), while the MGCP protocol uses client-server architecture, the calling scenario being very similar to the current PSTN/ISDN network.

After a call is setup, the voice streams transmit via RTP (Real-Time Transport Protocol). Different codecs (methods to compress and encode the voice) can be embedded into RTP packets. Vigor V models provide various codecs, including G.711 A/ μ -law, G.723, G.726 and G.729 A & B. Each codec uses a different bandwidth and hence provides different levels of voice quality. The more bandwidth a codec uses the better the voice quality, however the codec used must be appropriate for your Internet bandwidth.

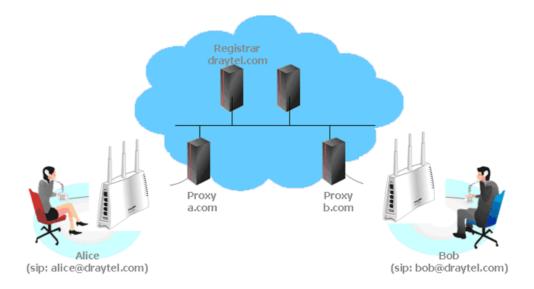
Usually there will be two types of calling scenario, as illustrated below:

• Calling via SIP Servers



First, the Vigor V models of yours will have to register to a SIP Registrar by sending registration messages to validate. Then, both parties' SIP proxies will forward the sequence of messages to caller to establish the session.

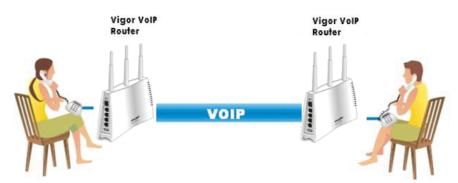
If you both register to the same SIP Registrar, then it will be illustrated as below:



The major benefit of this mode is that you don't have to memorize your friend's IP address, which might change very frequently if it's dynamic. Instead of that, you will only have to using **dial plan** or directly dial your friend's **account name** if you are with the same SIP Registrar. Please refer to the **section 4.5.1**.

Peer-to-Peer

Before calling, you have to know your friend's IP Address. The Vigor VoIP Routers will build connection between each other. Please refer to the **section 4.5.2**.



Our Vigor V models firstly apply efficient codecs designed to make the best use of available bandwidth, but Vigor V models also equip with automatic QoS assurance. QoS Assurance assists to assign high priority to voice traffic via Internet. You will always have the required inbound and outbound bandwidth that is prioritized exclusively for Voice traffic over Internet but you just get your data a little slower and it is tolerable for data traffic.





4.12.1 DialPlan

This page allows you to set phone book and digit map for the VoIP function. Click the **Phone Book** and **Digit Map** links on the page to access into next pages for dialplan settings.

VoIP >> DialPlan Setup

DialPlan Configuration

Phone Book	
<u>Digit Map</u>	
<u>Call Barring</u>	
Regional	
PSTN Setup	

Phone Book

VoIP >> DialPlan Setup

In this section, you can set your VoIP contacts in the "phonebook". It can help you to make calls quickly and easily by using "speed-dial" **Phone Number**. There are total 60 index entries in the phonebook for you to store all your friends and family members' SIP addresses. **Loop through** and **Backup Phone Number** will be displayed if you are using Vigor2110V for setting the phone book.

Index	Phone number	Display Name	SIP URL	Dial Out Account	Loop through	Backup Phone Number	Status
<u>1.</u>				Default	None		×
<u>2.</u>				Default	None		х
<u>3.</u>				Default	None		х
<u>4.</u>				Default	None		×
<u>5.</u>				Default	None		×
<u>6.</u>				Default	None		×
<u>7.</u>				Default	None		×
<u>8.</u>				Default	None		×
<u>9.</u>				Default	None		×
<u>10.</u>				Default	None		×
<u>11.</u>				Default	None		×
<u>12.</u>				Default	None		×
<u>13.</u>				Default	None		×
<u>14.</u>				Default	None		х
<u>15.</u>				Default	None		×
<u>16.</u>				Default	None		×
<u>17.</u>				Default	None		×
<u>18.</u>				Default	None		×
<u>19.</u>				Default	None		×
<u>20.</u>				Default	None		×

<< 1-20 | 21-40 | 41-60 >>

Status: v --- Active, x --- Inactive, ? --- Empty

<u>Next</u> >>



Click any index number to display the dial plan setup page.

VoIP >>	DialPlan	Setup
---------	----------	-------

🗹 Enable		
	Phone Number	1
	Display Name	Polly
	SIP URL	1112 @ fwd.pulver.com
	Dial Out Account	Default 💌
	Loop through	None 💌
	Backup Phone Number	

Enable	Click this to enable this entry.				
Phone Number	The speed-dial number of this index. This can be any number you choose, using digits 0-9 and * .				
Display Name	The Caller-ID that you want to be displayed on your friend's screen. This let your friend can easily know who's calling without memorizing lots of SIP URL Address.				
SIP URL	Enter your friend's SIP Address.				
Dial Out Account	Choose one of the SIP accounts for this profile to dial out. It is useful for both sides (caller and callee) that registered to different SIP Registrar servers. If caller and callee do not use the same SIP server, sometimes, the VoIP phone call connection may not succeed. By using the specified dial out account, the successful connection can be assured.				
Loop through	The selection should be as the following:				
	Loop through None Backup Phone Number PSTN				
Backup Phone Number	When the VoIP phone is obstructs or the Internet breaks down for some reasons, the backup phone will be dialed out to replace the VoIP phone number. At this time, the phone call will be changed from VoIP phone into PSTN call according to the loop through direction chosen. Note that, during the phone switch, the blare of phone will appear for a short time. And when the VoIP phone is switched into the PSTN phone, the telecom co. might charge you for the connection fee. Please type in backup phone number (PSTN) for this VoIP phone setting.				

Digit Map

For the convenience of user, this page allows users to edit prefix number for the SIP account with adding number, stripping number or replacing number. It is used to help user having a quick and easy way to dial out through VoIP interface.

Dig	it Map S	Setup						
#	Enable	Prefix Number	Mode	e	OP Number	Min Len	Max Len	Interface
1		03	Replace	*	8863	7	9	PSTN 🔽
2		886	Strip	~	886	8	10	PSTN 🔽
З			None	~		0	0	PSTN 🗸
4			None	~		0	0	PSTN 🔽
5			None	~		0	0	PSTN 🔽
6			None	~		0	0	PSTN 🔽
7			None	~		0	0	PSTN 🔽
8			None	~		0	0	PSTN 🔽
9			None	~		0	0	PSTN 🗸
10			None	~		0	0	PSTN 🔽
11			None	~		0	0	PSTN 🗸
12			None	~		0	0	PSTN 🔽
13			None	~		0	0	PSTN 🔽
14			None	~		0	0	PSTN 🔽
15			None	~		0	0	PSTN 🗸
16			None	~		0	0	PSTN 🔽
17			None	~		0	0	PSTN 🔽
18			None	~		0	0	PSTN 🔽
19			None	~		0	0	PSTN 🔽
20			None	~		0	0	PSTN 🔽

VoIP >> DialPlan Setup

Note: Min Len and Max Len should be between 0~25.

Enable	Check this box to invoke this setting.
Prefix Number	The phone number set here is used to add, strip, or replace the OP number.
Mode	 None - No action. Add - When you choose this mode, the OP number will be added with the prefix number for calling out through the specific VoIP interface. Strip - When you choose this mode, the OP number will be deleted by the prefix number for calling out through the specific VoIP interface. Take the above picture (Prefix Table Setup web page) as an example, the OP number of 886 will be deleted completely for the prefix number is set with 886. Replace - When you choose this mode, the OP number will be replaced by the prefix number for calling out through the specific VoIP interface. Take the above picture (Prefix Table Setup web page) as an example, the OP number of 886 will be deleted completely for the prefix number is set with 886.

Cancel

OK



Setup web page) as an example, the prefix number of 03 will be replaced by 8863. For example: dial number of "031111111" will be changed to "88631111111" and sent to SIP server. Mode

Replace	¥
None	
Add	
Strip	
Replace	

OP Number	The front number you type here is the first part of the account number that you want to execute special function (according to the chosen mode) by using the prefix number.
Min Len	Set the minimal length of the dial number for applying the prefix number settings. Take the above picture (Prefix Table Setup web page) as an example, if the dial number is between 7 and 9, that number can apply the prefix number settings here.
Max Len	Set the maximum length of the dial number for applying the prefix number settings.
Interface	Choose the one that you want to enable the prefix number settings from the saved SIP accounts. Please set up one SIP account first to make this interface available.

Call Barring

VoIP >> DialPlan Setup

Call barring is used to block phone calls coming from the one that is not welcomed.

Call Barring Setup					Set to Factory Default		
Index	Call Direction	Barring Type	Barring Number/URL/URI	Interface	Schedule	Status	
<u>1.</u>						x	
<u>2.</u>						x	
<u>3.</u>						х	
<u>4.</u>						х	
<u>5.</u>						x	
<u>6.</u>						х	
<u>7.</u>						х	
<u>8.</u>						x	
<u>9.</u>						x	
<u>10.</u>						×	

Advanced: <u>Block Anonymous</u> <u>Block Unknown Domain</u> <u>Block IP Address</u>

Click any index number to display the dial plan setup page.



VoIP >> DialPlan Setup

Call Barring Index No. 1	
Call Direction	IN 💌
Barring Type	Specific URI/URL 💌
Specific URI/URL	
Interface	All 💌
Index(1-15) in <u>Schedule</u> Setup	
1	
OK	Cancel

Click this to enable this entry.

Call Direction

Enable

Determine the direction for the phone call, IN - incoming call, OUT-outgoing call, IN & OUT - both incoming and outgoing calls.



Barring Type	Determine the type of the VoIP phone call, URI/URL or number. Specific URI/URL Specific URI/URL Specific Number
Specific URI/URL or Specific Number	This field will be changed based on the type you selected for barring Type.
Interface	All means all the phone calls will be blocked with such mechanism.
Index (1-15) in Schedule	Enter the index of schedule profiles to control the call barring according to the preconfigured schedules. Refer to section 3.5.2 Schedule for detailed configuration.

Additionally, you can set advanced settings for call barring such as **Block Anonymous**, **Block** Unknown Domain or Block IP Address. Simply click the relational links to open the web page.

For Block Anonymous - this function can block the incoming calls without caller ID on the interface (Phone port) specified in the following window. Such control also can be done based on preconfigured schedules.



VoIP >> DialPlan	Setup		
Call Barring Bloc	k Anonymous		
🔲 Enable			
Interfa	се	Phone1	Phone2
Index(3	1-15) in <u>Schedule</u> Setup	,,	
Note:Block the inc	coming calls which do not hav	e the caller ID.	
	OK	Cancel	

For **Block Unknown Domain** – this function can block incoming calls (through Phone port) from unrecognized domain that is not specified in SIP accounts. Such control also can be done based on preconfigured schedules.

VoIP >> [√olP >> DialPlan Setup		
Call Barr	ing Block Unknown Domain		
🗹 Enable	e		
	Interface	🗌 Phone1 🔲 Phone2	
	Index(1-15) in <u>Schedule</u> Setup		
Note:If the should be		ent from the domain found in SIP accounts,the call	
	OK	Cancel	

For **Block IP Address** – this function can block incoming calls (through Phone port) coming from IP address. Such control also can be done based on preconfigured schedules.

VoIP >> DialPlan Setup	
Call Barring Block IP Address	
🗹 Enable	
Interface	🗌 Phone1 🔲 Phone2
Index(1-15) in <u>Schedule</u> Setup	, , , , , , , , , , , , , , , , , , ,
Note: The incoming calls by means of IP dialing) (e.g.#192*168*1*1#) should be blocked.



Regional

This page allows you to process incoming or outgoing phone calls by regional. Default values (common used in most areas) will be shown on this web page. You *can change* the number based on the region that the router is placed.

VoIP >> DialPlan Setup

🗹 Enable Regional			Set to Factory Default
Last Call Return [Miss]:	*69		
Last Call Return [In]:	*12	Last Call Return [Out]:	*14
Call Forward [All] [Act]:	*72 +number+#	Call Forward [Deact]:	*73 +#
Call Forward [Busy] [Act]:	*90 +number+#	Call Forward [No Ans] [Act]:	*92 +number+#
Do Not Disturb [Act]:	*78 +#	Do Not Disturb [Deact]:	*79 +#
Hide caller ID [Act]:	*67 +#	Hide caller ID [Deact]:	*68 +#
Call Waiting [Act]:	*56 +#	Call Waiting [Deact]:	*57 +#
Block Anonymous [Act]:	*77 +#	Block Anonymous [Deact]:	*87 +#
Block Unknow Domain [Act]:	*40 +#	Block Unknow Domain [Deact]:	*04 +#
Block IP Calls [Act]:	*50 +#	Block IP Calls [Deact]:	*05 +#
Block Last Calls [Act]:	*60 +#		

OK		Cancel
----	--	--------

Last Call Return [Miss]	Sometimes, people might miss some phone calls. Please dial number typed in this field to know where the last phone call comes from and call back to that one.
Last Call Return [In]	You have finished an incoming phone call, however you want to call back again for some reason. Please dial number typed in this field to call back to that one.
Last Call Return [Out]	Dial the number typed in this field to call the previous outgoing phone call again.
Call Forward [All][Act]	Dial the number typed in this field to forward all the incoming calls to the specified place.
Call Forward [Deact]	Dial the number typed in this field to release the call forward function.
Call Forward [Busy][Act]	Dial the number typed in this field to forward all the incoming calls to the specified place while the phone is busy.
Call Forward [No Ans][Act]	Dial the number typed in this field to forward all the incoming calls to the specified place while there is no answer of the connected phone.
Do Not Disturb [Act]	Dial the number typed in this field to invoke the function of DND.



Do Not Distrub [Deact]	Dial the number typed in this field to release the DND function.
Hide caller ID [Act]	Dial the number typed in this field to make your phone number (ID) not displayed on the display panel of remote end.
Hide caller ID [Deact]	Dial the number typed in this field to release this function.
Call Waiting [Act]	Dial the number typed in this field to make all the incoming calls waiting for your answer.
Call Waiting [Deact]	Dial the number typed in this field to release this function.
Block Anonymous[Act]	Dial the number typed in this field to block all the incoming calls with unknown ID.
Block Anonymous[Deact]	Dial the number typed in this field to release this function.
Block Unknown Domain [Act]	Dial the number typed in this field to block all the incoming calls from unknown domain.
Block Unknown Domain [Deact]	Dial the number typed in this field to release this function.
Block IP Calls [Act]	Dial the number typed in this field to block all the incoming calls from IP address.
Block IP Calls [Deact]	Dial the number typed in this field to release this function.
Block Last Calls [Act]	Dial the number typed in this field to block the last incoming phone call.

PSTN Setup

Some emergency phone (e.g., 911) or special phone cannot be dialed out by using VoIP and can be called out through PSTN line only. To solve this problem, this page allows you to set five sets of PSTN number for dialing without passing through Internet. Please type the number in the field of **phone number for PSTN relay**.

Enable	phone number for PSTN relay

VoIP >> PSTN Setup

Then, check the **Enable** box to make the PSTN number available for dial whenever you need.



4.12.2 SIP Accounts

In this section, you set up your own SIP settings. When you apply for an account, your SIP service provider will give you an **Account Name** or user name, **SIP Registrar, Proxy,** and **Domain name**. (The last three might be the same in some case). Then you can tell your folks your SIP Address as in **Account Name@ Domain name**

As Vigor VoIP Router is turned on, it will first register with Registrar using AuthorizationUser@Domain/Realm. After that, your call will be bypassed by SIP Proxy to the destination using AccountName@Domain/Realm as identity.

VoIP >>	SIP Acc	ounts					
SIP Acc	ounts Lis	t					Refresh
Index	Profile	Domain/Realm	Proxy	Account Name	Ring	g Port	Status
1					Phone1	Phone2	-
2					Phone1	Phone2	-
<u>3</u>					Phone1	Phone2	-
<u>4</u>					Phone1	Phone2	-
<u>5</u>					Phone1	Phone2	-
<u>6</u>					Phone1	Phone2	-
						egistered on S ster on SIP se	
NAT Tra	versal Se	etting					
	STUN S	Gerver:					

STUN Server:	
External IP:	
SIP PING Interval:	150 sec

_		_
	OK	

Index	Click this link to access into next page for setting SIP account.
Profile	Display the profile name of the account.
Domain/Realm	Display the domain name or IP address of the SIP registrar server.
Proxy	Display the domain name or IP address of the SIP proxy server.
Account Name	Display the account name of SIP address before @.
Ring Port	Specify which port will ring when receiving a phone call.
STUN Server	Type in the IP address or domain of the STUN server.
External IP	Type in the gateway IP address.
SIP PING interval	The default value is 150 (sec). It is useful for a Nortel server NAT Traversal Support.
Status	Show the status for the corresponding SIP account. R means such account is registered on SIP server successfully. – means the account is failed to register on SIP server.

VoIP >> SIP Accounts

SIP Account Index No. 1

Profile Name	(11 char max.)
Register via	None 🔽 🔲 Call without Registration
SIP Port	5060
Domain/Realm	(63 char max.)
Proxy	(63 char max.)
Act as outbound pro-	y
Display Name	(23 char max.)
Account Number/Name	(63 char max.)
Authentication ID	(63 char max.)
Password	(63 char max.)
Expiry Time	1 hour 💙 3600 sec
NAT Traversal Support	None 💌
Ring Port	Phone 1 Phone 2
Ring Pattern	1 💌
	OK Cancel

Profile Name	Assign a name for this profile for identifying. You can type similar name with the domain. For example, if the domain name is <i>draytel.org</i> , then you might set <i>draytel-1</i> in this field.
Register via	If you want to make VoIP call without register personal information, please choose None and check the box to achieve the goal. Some SIP server allows user to use VoIP function without registering. For such server, please check the box of Call without Registration . Choosing Auto is recommended. The system will select a proper way for your VoIP call. Register via None Auto WAN1 LAN/VPN SIP PortSet the port number for sending/receiving SIP message for building a session. The default value is 5060 . Your peer must set the same value in his/her Registrar.
Domain/Realm	Set the domain name or IP address of the SIP Registrar server.
Proxy	Set domain name or IP address of SIP proxy server. By the time you can type :port number after the domain name to specify that port as the destination of data transmission (e.g., nat.draytel.org:5065)
Act as Outbound Proxy	Check this box to make the proxy acting as outbound proxy.
Display Name	The caller-ID that you want to be displayed on your friend's screen.
Account Number/Name	Enter your account name of SIP Address, e.g. every text before @.
Authentication ID	Check the box to invoke this function and enter the name or number used for SIP Authorization with SIP Registrar. If this



	setting value is the same as Account Name, it is not necessary for you to check the box and set any value in this field.					
Password	The password provided to you when you registered with a SIP service.					
Expiry Time	The time duration that your SIP Registrar server keeps your registration record. Before the time expires, the router will send another register request to SIP Registrar again.					
NAT Traversal Support	If the router (e.g., broadband router) you use connects to internet by other device, you have to set this function for your necessity.					
	NAT Traversal Support None None Stun Manual Nortel					
	 None – Disable this function. Stun – Choose this option if there is Stun server provided for your router. Manual – Choose this option if you want to specify an external IP address as the NAT transversal support. Nortel – If the soft-switch that you use supports Nortel solution, you can choose this option. 					
Ring Port	Set Phone1 or Phone2 as the default ring port for this SIP account.					
Ring Pattern	Choose a ring tone type for the VoIP phone call. Ring Pattern 1 2 3 4 5 6					

4.12.3 Phone Settings

This page allows user to set phone settings for Phone 1 and Phone 2 respectively. However, it changes slightly according to different model you have.

Phone	LIST						
Index	Port	Call Feature	Codec	Tone	Gain (Mic/Speaker)	Default SIP Account	DTMF Relay
1	Phone1	CW,CT,	G.729A/B	User Defined	5/5		InBand
2	Phone2	CW,CT,	G.729A/B	User Defined	5/5		InBand
лтр							
	🗌 Syr	nmetric RTP					
	Dynami	c RTP Port S	Start	10050			
Dynamic RTP Port End				15000			
	RTP TC	S		IP preced	dence 5 🔽 🚺	0100000	

Phone List Port – there are two phone ports provided here for you to configure. Phone1/Phone2 allow you to set general settings for PSTN phones. Call Feature – A brief description for call feature will be shown in this field for your reference. **Codec** – The default Codec setting for each port will be shown in this field for your reference. You can click the number below the Index field to change it for each phone port. Tone - Display the tone settings that configured in the advanced settings page of Phone Index. Gain - Display the volume gain settings for Mic/Speaker that configured in the advanced settings page of Phone Index. **Default SIP Account** – "draytel_1" is the default SIP account. You can click the number below the Index field to change SIP account for each phone port. DTMF Relay – Display DTMF mode that configured in the advanced settings page of Phone Index. RTP Symmetric RTP – Check this box to invoke the function. To make the data transmission going through on both ends of local router and remote router not misleading due to IP lost (for example, sending data from the public IP of remote router to the private IP of local router), you can check this box to solve this problem. Dynamic RTP Port Start - Specifies the start port for RTP stream. The default value is 10050. Dynamic RTP Port End - Specifies the end port for RTP stream. The default value is 15000. **RTP TOS** – It decides the level of VoIP package. Use the drop

down list to choose any one of them.

Manual
Iviariual
IP precedence 1
IP precedence 2
IP precedence 3
IP precedence 4
IP precedence 5
IP precedence 6
IP precedence 7
AF Class1 (Low Drop)
AF Class1 (Medium Drop)
AF Class1 (High Drop)
AF Class2 (Low Drop)
AF Class2 (Medium Drop)
AF Class2 (High Drop)
AF Class3 (Low Drop)
AF Class3 (Medium Drop)
AF Class3 (High Drop)
AF Class4 (Low Drop)
AF Class4 (Medium Drop)
AF Class4 (High Drop)
EF Class
Manual

RTP TOS

Detailed Settings for Phone Port

Click the number link for Phone port, you can access into the following page for configuring Phone settings.

VoIP >> Phone Settings

Phone1				
Call Feature			Codecs	
🔲 Hotline			Prefer Codec	G.729A/B (8Kbps) 💌
Session Timer	90	sec		Single Codec
Call Forwarding	Disable 🛛 👻		Packet Size	20ms 🚩
SIP URL			Voice Active Detector	Off 🔽
Time Out	30 sec		Default SIP Account	
🔲 DND(Do Not Disturb) Mode			
Index(1-15) in Sc	·		Play dial tone only t	when account registered
Note: Action and be ignored	d Idle Timeout sett 1.	ings will		
Index(1-60) in <u>Ph</u>	one Book as Excep	tion List:		
CLIR (hide caller ID))			
🗹 Call Waiting				
🗹 Call Transfer				
	ОК	Car	ncel Advanced	
Iotline			to enable it. Type in tically when you pic	the SIP URL in the field f k up the phone set.
Session Timer	you se	t in this i		on. In the limited time that esponse, the connecting cal
Call Forwarding	forwar	ding fun	ction. Always mean	noose. Disable is to close c s all the incoming calls will t any reason. Busy means

the incoming calls will be forwarded into SIP URL only when the local system is busy. **No Answer** means if the incoming calls do not receive any response, they will be forwarded to the SIP URL by the time out.

	Disable
	Disable
	Always Busy
	No Answer SIP URL – Type in the SIP URL (e.g., aaa@draytel.org or
	abc@iptel.org) as the site for call forwarded.
	Time Out – Set the time out for the call forwarding. The default setting is 30 sec.
DND (Do Not Disturb) mode	Set a period of peace time without disturbing by VoIP phone call. During the period, the one who dial in will listen busy tone, yet the local user will not listen any ring tone.
	Index (1-15) in Schedule - Enter the index of schedule profiles to control the DND mode according to the preconfigured schedules. Refer to section 3.8.2 Schedule for detailed configuration.
	Index (1-60) in Phone Book - Enter the index of phone book profiles. Refer to section 3.11.1 DialPlan – Phone Book for detailed configuration.
CLIR (hide caller ID)	Check this box to hide the caller ID on the display panel of the phone set.
Call Waiting	Check this box to invoke this function. A notice sound will appear to tell the user new phone call is waiting for your response. Click hook flash to pick up the waiting phone call.
Call Transfer	Check this box to invoke this function. Click hook flash to initiate another phone call. When the phone call connection succeeds, hang up the phone. The other two sides can communicate, then.
Prefer Codec	Salast one of five codess as the default for your VoID calls. The
	Select one of five codecs as the default for your VoIP calls. The codec used for each call will be negotiated with the peer party before each session, and so may not be your default choice. The default codec is G.729A/B; it occupies little bandwidth while maintaining good voice quality. If your upstream speed is only 64Kbps, do not use G.711 codec.
	codec used for each call will be negotiated with the peer party before each session, and so may not be your default choice. The default codec is G.729A/B; it occupies little bandwidth while maintaining good voice quality. If your upstream speed is only 64Kbps, do not use G.711 codec. It is better for you to have at least 256Kbps upstream if you would like to use G.711.
	codec used for each call will be negotiated with the peer party before each session, and so may not be your default choice. The default codec is G.729A/B; it occupies little bandwidth while maintaining good voice quality. If your upstream speed is only 64Kbps, do not use G.711 codec. It is better for you to have at least 256Kbps upstream if you would like to use G.711. Prefer Codec G.711A (64Kbps)
	codec used for each call will be negotiated with the peer party before each session, and so may not be your default choice. The default codec is G.729A/B; it occupies little bandwidth while maintaining good voice quality. If your upstream speed is only 64Kbps, do not use G.711 codec. It is better for you to have at least 256Kbps upstream if you would like to use G.711.
	codec used for each call will be negotiated with the peer party before each session, and so may not be your default choice. The default codec is G.729A/B; it occupies little bandwidth while maintaining good voice quality. If your upstream speed is only 64Kbps, do not use G.711 codec. It is better for you to have at least 256Kbps upstream if you would like to use G.711. Prefer Codec G.711A (64Kbps) G.711A (64Kbps) G.711A (64Kbps) G.729A/B (8Kbps)
	codec used for each call will be negotiated with the peer party before each session, and so may not be your default choice. The default codec is G.729A/B; it occupies little bandwidth while maintaining good voice quality. If your upstream speed is only 64Kbps, do not use G.711 codec. It is better for you to have at least 256Kbps upstream if you would like to use G.711. Prefer Codec G.711A (64Kbps) G.711A (64Kbps) G.711A (64Kbps)

Single Codec – If the box is checked, only the selected Codec will be applied.

Packet Size-The amount of data contained in a single packet. The default value is 20 ms, which means the data packet will contain 20 ms voice information. Packet Size



Voice Active Detector - This function can detect if the voice on both sides is active or not. If not, the router will do something to save the bandwidth for other using. Click On to invoke this function; click off to close the function.

Voice Active Detector



Default SIP AccountYou can set SIP accounts (up to six groups) on SIP Account
page. Use the drop down list to choose one of the profile names
for the accounts as the default one for this phone setting.

Play dial tone only when account registered - Check this box to invoke the function.

In addition, you can press the **Advanced** button to configure tone settings, volume gain, MISC and DTMF mode. **Advanced** setting is provided for fitting the telecommunication custom for the local area of the router installed. Wrong tone settings might cause inconvenience for users. To set the sound pattern of the phone set, simply choose a proper region to let the system find out the preset tone settings and caller ID type automatically. Or you can adjust tone settings manually if you choose User Defined. TOn1, TOff1, TOn2 and TOff2 mean the cadence of the tone pattern. TOn1 and TOn2 represent sound-on; TOff1 and TOff2 represent the sound-off.

Tone Se	ttings						
Region	User Defined	*		Ca	ller ID Type	FSK_ETSI	1
		Low Freq (Hz)	High Freq (Hz)	T on 1 (msec)	T off 1 (msec)	T on 2 (msec)	T off 2 (msec)
Die	al tone	350	440	0	0	0	0
Ring	ing tone	400	450	400	200	400	2000
Busy tone 400		400	0	375	375	0	0
Conge	stion tone	0	0	0	0	0	0
Volume	Gain			DTMF			
Mic Gain	(1-10)	5		DTMF Mo	de	InBand	~
Speaker Gain(1-10)		5		Payload T	ype(RFC2833) 101	
MISC							
Dial Tone	e Power Level	l (1 - 50) 2	7				
Ring Free	quency (10 -	50HZ) 25	5				

VoIP >> Phone Settings

Region

Select the proper region which you are located. The common settings of **Caller ID Type**, **Dial tone**, **Ringing tone**, **Busy tone** and **Congestion tone** will be shown automatically on the page. If you cannot find out a suitable one, please choose **User**



Defined and fill out the corresponding values for dial tone, ringing tone, busy tone, congestion tone by yourself for VoIP phone.

	nurance county as a more
	Tone Settings
	Region User Defined 🕶
	User Defined
	Dia Denmark i0
	Ringi Italy 0
	Germany Bus Netherlands
	Conges
	Volume (Australia
	Mic Gain(Slovenia
	Uzech
	Speaker (Slovakia Hungary
	MISC Switzerland
	Dial Tone Power Level (1 - 50
	Also, you can specify each field for your necessity. It is
	recommended for you to use the default settings for VoIP
	communication.
Volume Gain	Mic Gain (1-10)/Speaker Gain (1-10) - Adjust the volume of microphone and speaker by entering number from 1- 10. The larger of the number, the louder the volume is.
MISC	Dial Tone Power Level - This setting is used to adjust the loudness of the dial tone. The smaller the number is, the louder the dial tone is. It is recommended for you to use the default setting.Ring Frequency - This setting is used to drive the frequency of the ring tone. It is recommended for you to use the default setting.
DTMF	 DTMF Mode – There are four DTMF modes for you to choose. <i>InBand</i> - Choose this one then the Vigor will send the DTMF tone as audio directly when you press the keypad on the phone <i>OutBand</i> - Choose this one then the Vigor will capture the keypad number you pressed and transform it to digital form then send to the other side; the receiver will generate the tone according to the digital form it receive. This function is very useful when the network traffic congestion occurs and it still can remain the accuracy of DTMF tone. <i>SIP INFO</i>- Choose this one then the Vigor will capture the DTMF tone and transfer it into SIP form. Then it will be sent to the remote end with SIP message.
	DTMF mode InBand 💙

InBand OutBand (RFC2833) SIP INFO (cisco format) SIP INFO (nortel format)

Payload Type (rfc2833) - Choose a number from 96 to 127,

the default value was 101. This setting is available for the OutBand (RFC2833) mode.

4.12.4 Status

VoIP >> Status

From this page, you can find codec, connection and other important call status for each port.

Status								Refres	n Seco	nds:	10 🚩	Refresh
Port	Status	Codec	PeerID	Elapse (hh:mm:ss)	Tx Pkts	Rx Pkts	Rx Losts	Rx Jitter (ms)	In Calls	Out Calls		Speake Gain
Phone1	IDLE			00:00:00	0	0	0	0	0	0	0	5
Phone2	IDLE			00:00:00	0	0	0	0	0	0	0	5
(mm-dd-yyyy) (hh:mm:ss)		(hh:mm:s	з)									
Date		Time		Duration	I	n/Out	/Miss	Acc	ount	ID	Peer	ID
			3)									
00-00-	0	00:00:		00:00:00	-			-				
00-00-	0	00:00:	:00	00:00:00	-			-				
00-00-	0	00:00:	:00	00:00:00	-			-				
00-00-	0	00:00:	:00	00:00:00	-			-				
00-00-	0	00:00:	:00	00:00:00	-			-				
00-00-	0	00:00:	:00	00:00:00	-			-				
00-00-	0	00:00:	:00	00:00:00	-			-				
00-00-	0	00:00:	:00	00:00:00	-			-				
00-00-	0	00:00:	:00	00:00:00	-			-				
00-00-	Ο	00:00:	00	00:00:00	_			_				

Refresh Seconds Specify the interval of refresh time to obtain the latest VoIP calling information. The information will update immediately when the Refresh button is clicked.



Port	It shows current connection status for the port of Phone1 and Phone2.
Status	It shows the VoIP connection status. IDLE - Indicates that the VoIP function is idle. HANG_UP - Indicates that the connection is not established (busy tone). CONNECTING - Indicates that the user is calling out. WAIT_ANS - Indicates that a connection is launched and waiting for remote user's answer. ALERTING - Indicates that a call is coming. ACTIVE-Indicates that the VoIP connection is launched.
Codec	Indicates the voice codec employed by present channel.
PeerID	The present in-call or out-call peer ID (the format may be IP or Domain).
Elapse	The format is represented as hours:minutes:seconds.
Tx Pkts	Total number of transmitted voice packets during this connection session.



Rx Pkts	Total number of received voice packets during this connection session.
Rx Losts	Total number of lost packets during this connection session.
Rx Jitter	The jitter of received voice packets.
In Calls	Accumulation for the times of in call.
Out Calls	Accumulation for the times of out call.
Miss Calls	Accumulation for the times of missing call.
Speaker Gain	The volume of present call.
Log	Display logs of VoIP calls.

4.13 Wireless LAN

This function is used for "n" models only.

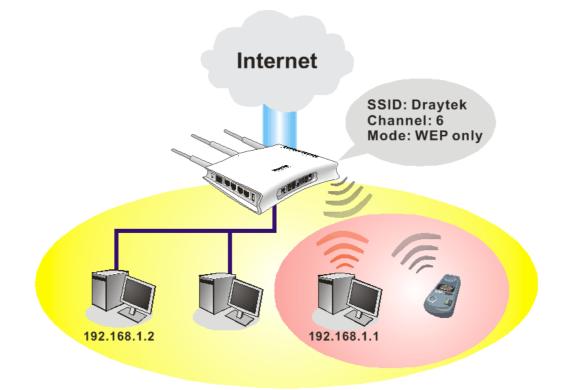
4.13.1 Basic Concepts

Over recent years, the market for wireless communications has enjoyed tremendous growth. Wireless technology now reaches or is capable of reaching virtually every location on the surface of the earth. Hundreds of millions of people exchange information every day via wireless communication products. The Vigor "n" model, a.k.a. Vigor wireless router, is designed for maximum flexibility and efficiency of a small office/home. Any authorized staff can bring a built-in WLAN client PDA or notebook into a meeting room for conference without laying a clot of LAN cable or drilling holes everywhere. Wireless LAN enables high mobility so WLAN users can simultaneously access all LAN facilities just like on a wired LAN as well as Internet access.

The Vigor wireless routers are equipped with a wireless LAN interface compliant with the standard IEEE 802.11n draft 2 protocol. To boost its performance further, the Vigor Router is also loaded with advanced wireless technology to lift up data rate up to 300 Mbps*. Hence, you can finally smoothly enjoy stream music and video.

Note: * The actual data throughput will vary according to the network conditions and environmental factors, including volume of network traffic, network overhead and building materials.

In an Infrastructure Mode of wireless network, Vigor wireless router plays a role as an Access Point (AP) connecting to lots of wireless clients or Stations (STA). All the STAs will share the same Internet connection via Vigor wireless router. The **General Settings** will set up the information of this wireless network, including its SSID as identification, located channel etc.



Multiple SSIDs

Vigor router supports four SSID settings for wireless connections. Each SSID can be defined with different name and download/upload rate for selecting by stations connected to the router wirelessly.

Security Overview

Real-time Hardware Encryption: Vigor Router is equipped with a hardware AES encryption engine so it can apply the highest protection to your data without influencing user experience.

Complete Security Standard Selection: To ensure the security and privacy of your wireless communication, we provide several prevailing standards on market.

WEP (Wired Equivalent Privacy) is a legacy method to encrypt each frame transmitted via radio using either a 64-bit or 128-bit key. Usually access point will preset a set of four keys and it will communicate with each station using only one out of the four keys.

WPA (Wi-Fi Protected Access), the most dominating security mechanism in industry, is separated into two categories: WPA-personal or called WPA Pre-Share Key (WPA/PSK), and WPA-Enterprise or called WPA/802.1x.

In WPA-Personal, a pre-defined key is used for encryption during data transmission. WPA applies Temporal Key Integrity Protocol (TKIP) for data encryption while WPA2 applies AES. The WPA-Enterprise combines not only encryption but also authentication.

Since WEP has been proved vulnerable, you may consider using WPA for the most secure connection. You should select the appropriate security mechanism according to your needs. No matter which security suite you select, they all will enhance the over-the-air data protection and /or privacy on your wireless network. The Vigor wireless router is very flexible and can support multiple secure connections with both WEP and WPA at the same time.

Separate the Wireless and the Wired LAN- WLAN Isolation enables you to isolate your wireless LAN from wired LAN for either quarantine or limit access reasons. To isolate means neither of the parties can access each other. To elaborate an example for business use, you



may set up a wireless LAN for visitors only so they can connect to Internet without hassle of the confidential information leakage. For a more flexible deployment, you may add filters of MAC addresses to isolate users' access from wired LAN.

Manage Wireless Stations - Station List will display all the station in your wireless network and the status of their connection.

Below shows the menu items for Wireless LAN.

Wireless LAN
• WPS
* WDS
 WMM Configuration
AP Discovery

4.13.2 General Setup

By clicking the **General Settings**, a new web page will appear so that you could configure the SSID and the wireless channel. Please refer to the following figure for more information.

al Setting			
able Wirele	ss LAN		
Mode :		Mixed(11b+11g	j+11n) 🔽
Index(1-1	5) in <u>Schedule</u>	Setup: ,	
	dule profiles tha ons are ignored	at have the action "Force Down"	are applied to the WLAN, all
Enable	Hide SSID	SSID	Isolate LAN Member
1		DrayTek	
2			
3 🔲			
4			
Isolate M other. Isolate L LAN.	lember:Wireles	o from being scanned. Is clients (stations) with the sam ents (stations) with the same SS MHz	SID cannot access wired PCs or
Isolate M other. Isolate L LAN. Channel: [Long Preat	lember:Wireless AN:Wireless clia Channel 6, 2437M mble: necessary YERDRIVE TM	s clients (stations) with the sam	SID cannot access wired PCs on
Isolate M other. Isolate L LAN. Channel: [Long Preat Packet-ON D Tx Bur Note:	Iember:Wireless AN:Wireless clie Channel 6, 2437N mble: necessary /ERDRIVE TM st	es clients (stations) with the same SS ents (stations) with the same SS MHz	SID cannot access wired PCs on e: only(lower performance)
Isolate M other. Isolate L LAN. Channel: [Long Preat Packet-ON D Tx Bur Note:	Iember:Wireless AN:Wireless clia Channel 6, 2437M mble: necessary VERDRIVE TM st technology mu: rol	is clients (stations) with the same SS ents (stations) with the same SS //Hz y for some old 802.11 b devices st also be supported in clients to	SID cannot access wired PCs on e: only(lower performance) o boost WLAN performance.
Isolate M other. Isolate L LAN. Channel: [Long Preat Packet-OV A Tx Bur Note: The same Rate Cont	Iember:Wireless AN:Wireless clie Channel 6, 2437M mble: necessary YERDRIVE TM st technology mu: rol Enable	The series of the series of the series of the series (stations) with the series of the	SID cannot access wired PCs on e: only(lower performance) o boost WLAN performance.
Isolate M other. Isolate L LAN. Channel: [Long Preat Packet-OV Tx Bur Note: The same Rate Cont	Iember:Wireless AN:Wireless clia Channel 6, 2437M mble: necessary /ERDRIVE [™] st technology mu: rol Enable	s clients (stations) with the same ents (stations) with the same SS <u>AHz</u> Long Preamble y for some old 802.11 b devices of st also be supported in clients to <u>Upload</u> <u>30000</u> kbps	SID cannot access wired PCs on e: only(lower performance) o boost WLAN performance. Download 30000 kbps
Isolate M other. Isolate L LAN. Channel: [Long Preat Packet-OV A Tx Bur Note: The same Rate Cont	Iember:Wireless AN:Wireless clia Channel 6, 2437M mble: necessary /ERDRIVE TM st technology mu: rol Enable	s clients (stations) with the same ents (stations) with the same SS AHz Long Preamble y for some old 802.11 b devices of st also be supported in clients to Upload 30000 kbps 30000 kbps	SID cannot access wired PCs on e: only(lower performance) b boost WLAN performance. Download 30000 kbps 30000 kbps
Isolate M other. Isolate L LAN. Channel: [Long Pread Packet-OV D Tx Bur Note: The same Rate Cont SSID 1 SSID 2	Iember:Wireless AN:Wireless clie Channel 6, 2437M mble: necessary YERDRIVE TM st technology mu: rol Enable	s clients (stations) with the same ents (stations) with the same SS AHz Long Preamble y for some old 802.11 b devices of st also be supported in clients to Upload 30000 kbps 30000 kbps	SID cannot access wired PCs on e: only(lower performance) b boost WLAN performance. Download 30000 kbps 30000 kbps

Enable Wireless LAN Mode Check the box to enable wireless function.

At present, the router can connect to Mixed (11b+11g), 11g Only, 11b Only, Mixed (11g+11n), 11n Only and Mixed (11b+11g+11n) stations simultaneously. Simply choose Mix (11b+11g+11n) mode.

Mixed(11b+11g+11n) 11b Only 11g Only 11n Only Mixed(11b+11g) Mixed(11g+11n) Mixed(11b+11g+11n)

	Note: You should also set RADIUS Server simultaneously if 11g Only, 11b Only or 11n Only mode is selected.	
Index(1-15)	Set the wireless LAN to work at certain time interval only. You may choose up to 4 schedules out of the 15 schedules pre-defined in Applications >> Schedule setup. The default setting of this field is blank and the function will always work.	
Hide SSID	Check it to prevent from wireless sniffing and make it harder for unauthorized clients or STAs to join your wireless LAN. Depending on the wireless utility, the user may only see the information except SSID or just cannot see any thing about Vigor wireless router while site surveying. The system allows you to set four sets of SSID for different usage. In default, the first set of SSID will be enabled. You can hide it for your necessity.	
SSID	Means the identification of the wireless LAN. SSID can be any text numbers or various special characters. The default SSID is "Draytek. We suggest you to change it.	
Isolate	 LAN – Check this box to make the wireless clients (stations) with the same SSID cannot access wired PCs on LAN. Member –Check this box to make the wireless clients (stations) with the same SSID not accessing for each other. 	
Channel	Means the channel of frequency of the wireless LAN. The default channel is 6. You may switch channel if the selected channel is under serious interference. If you have no idea of choosing the frequency, please select Auto to let system determine for you.	
	Channel: Channel 6, 2437MHz Auto Channel 1, 2412MHz Channel 2, 2417MHz Channel 3, 2422MHz Channel 4, 2427MHz Channel 5, 2432MHz Channel 6, 2437MHz Channel 6, 2437MHz Channel 7, 2442MHz Channel 8, 2447MHz Channel 9, 2452MHz Channel 10, 2457MHz Channel 11, 2462MHz Channel 12, 2467MHz Channel 13, 2472MHz	
Long Preamble	This option is to define the length of the sync field in an 802.11 packet. Most modern wireless network uses short preamble with 56 bit sync field instead of long preamble with 128 bit sync field. However, some original 11b wireless network devices only support long preamble.	

Check it to use **Long Preamble** if needed to communicate with this kind of devices.

Packet-OVERDRIVE

This feature can enhance the performance in data transmission about 40%* more (by checking **Tx Burs**t). It is active only when both sides of Access Point and Station (in wireless client) invoke this function at the same time. That is, the wireless client must support this feature and invoke the function, too.

Note: Vigor N61 wireless adapter supports this function. Therefore, you can use and install it into your PC for matching with Packet-OVERDRIVE (refer to the following picture of Vigor N61 wireless utility window, choose **Enable** for **TxBURST** on the tab of **Option**).

- Advance Setting		
Disable <u>R</u> adio		
<u>Fragmentation</u> Threshold :	23	346
RTS Threshold :	23	347
Frequency :	802.11b/g/n - 2.4GH	*
Ad-hoc <u>C</u> hannel:	1	~
Power Save Mode:	Disable	~
Tx <u>B</u> urst :	Disable	*
OK (Cancel	pply
	Disable Radio Eragmentation Threshold : RTS Threshold : Frequency : Ad-hoc Channel: Power Save Mode: Tx Eurst :	Disable Redio Eragmentation Threshold : 23 RTS Threshold : 23 Frequency : 802.11b/g/n - 2.4GH Ad-hoc Channel: 1 Poyer Save Mode: Disable Tx Eurst : Disable

Rate Control

It controls the data transmission rate through wireless connection.

Upload – Check Enable and type the transmitting rate for data upload. Default value is 30,000 kbps.

Download – Type the transmitting rate for data download. Default value is 30,000 kbps.

4.13.3 Security

This page allows you to set security with different modes for SSID 1, 2, 3 and 4 respectively. After configuring the correct settings, please click **OK** to save and invoke it.

By clicking the **Security Settings**, a new web page will appear so that you could configure the settings of WEP and WPA.

SSI	ID 1 SSID 2	SSID 3	SSID 4	
	Mode:		Disable	~
	WPA:			
	Encryption Mode:		TKIP for WPA/AES f	for WPA2
	Pre-Shared Key		******	
	Type 8~63 AS0 "cfgs01a2" of			ts leading by "0x", for example
	WEP:			
	Encryption Mod	e:	64-Bit 🗸	
	• Key 1 :		*****	
	○Key 2 :		*****	

	○Key 3 :			
	○Key 4 :		******	
	For 128 bit WEP key Type 13 ASCII charac "0123456789abc" or "	ter or 26 Hexa		by "0x", for example
			OK Cancel	
Iode		Th	ere are several me	odes provided for you to choose.
		М	ode:	Disable 💌
				Disable
				WEP WPA/PSK
				WPA2/PSK
		D:	ashla Tuma off 4	Mixed(WPA+WPA2)/PSK
				he encryption mechanism. WEP clients and the encryption key
			ould be entered in	
				s only WPA clients and the encrypti-
			y should be entered	
			•	ts only WPA2 clients and the
		en	cryption key shou	ld be entered in PSK.
				A2)/PSK - Accepts WPA and WPA
			ents simultaneous tered in PSK.	sly and the encryption key should be
VPA		Th	e WPA encrypts	each frame transmitted from the rad
			• •	h either PSK (Pre-Shared Key) enter
				d below or automatically negotiated
				cation. Either 8~63 ASCII character

Wireless LAN >> Security Settings



such as 012345678(or 64 Hexadecimal digits leading by 0x,

such as "0x321253abcde..."). **Type** - Select from Mixed (WPA+WPA2) or WPA2 only. **Pre-Shared Key (PSK)** - Either **8~63** ASCII characters, such as 012345678..(or 64 Hexadecimal digits leading by 0x, such as "0x321253abcde...").

64-Bit - For 64 bits WEP key, either **5** ASCII characters, such as 12345 (or 10 hexadecimal digitals leading by 0x, such as 0x4142434445.) **128-Bit** - For 128 bits WEP key, either **13** ASCII characters, such as ABCDEFGHIJKLM (or 26

hexadecimal digits leading by 0x, such as 0x4142434445464748494A4B4C4D).

Encryption Mode:

	64-Bit	*
	64-Bit	
	128-Bit	
h	e same V	VE

All wireless devices must support the same WEP encryption bit size and have the same key. **Four keys** can be entered here, but only one key can be selected at a time. The keys can be entered in ASCII or Hexadecimal. Check the key you wish to use.

4.13.4 Access Control

WEP

For additional security of wireless access, the **Access Control** facility allows you to restrict the network access right by controlling the wireless LAN MAC address of client. Only the valid MAC address that has been configured can access the wireless LAN interface. By clicking the **Access Control**, a new web page will appear, as depicted below, so that you could edit the clients' MAC addresses to control their access rights.

Enable Mac A	ddress Filter	
🔲 SSII	1 SSID 2 SSID 3	SSID 4
	MAC Address Filter	
Index	Attribute MAC Address	
Client	s MAC Address : : : :]: [] : []
	Attribute :	
	📃 s: Isolate the station from I	LAN
	Add Delete Edit	Cancel

Wireless LAN >> Access Control

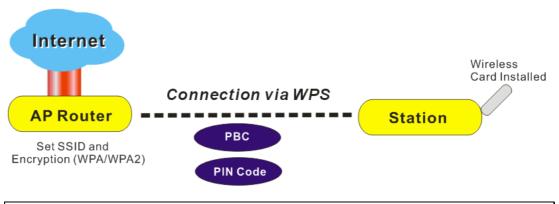


Select to enable the MAC Address filter for wireless LAN identified with SSID 1 to 4 respectively. All the clients (expressed by MAC addresses) listed in the box can be grouped under different wireless LAN. For example, they

	can be grouped under SSID 1 and SSID 2 at the same time if you check SSID 1 and SSID 2.
MAC Address Filter	Display all MAC addresses that are edited before.
Client's MAC Address	Manually enter the MAC address of wireless client.
Attribute	s: Isolate the station from LAN - select to isolate the wireless connection of the wireless client of the MAC address from LAN.
Add	Add a new MAC address into the list.
Delete	Delete the selected MAC address in the list.
Edit	Edit the selected MAC address in the list.
Cancel	Give up the access control set up.
ОК	Click it to save the access control list.
Clear All	Clean all entries in the MAC address list.

4.13.5 WPS

WPS (Wi-Fi Protected Setup) provides easy procedure to make network connection between wireless station and wireless access point (vigor router) with the encryption of WPA and WPA2.

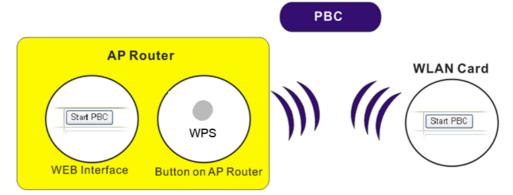


Note: Such function is available for the wireless station with WPS supported.

It is the simplest way to build connection between wireless network clients and vigor router. Users do not need to select any encryption mode and type any long encryption passphrase to setup a wireless client every time. He/she only needs to press a button on wireless client, and WPS will connect for client and router automatically.

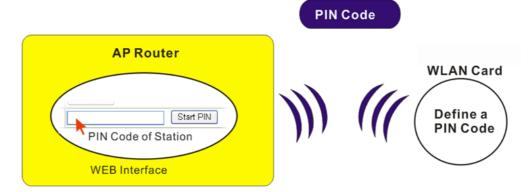
There are two methods to do network connection through WPS between AP and Stations: pressing the *Start PBC* button or using *PIN Code*.

• On the side of Vigor 2110 series which served as an AP, press **WPS** button once on the front panel of the router or click **Start PBC** on web configuration interface. On the side



of a station with network card installed, press Start PBC button of network card.

• If you want to use PIN code, you have to know the PIN code specified in wireless client. Then provide the PIN code of the wireless client you wish to connect to the vigor router.



For WPS is supported in WPA-PSK or WPA2-PSK mode, if you do not choose such mode in **Wireless LAN>>Security**, you will see the following message box.



Please click **OK** and go back **Wireless LAN>>Security** to choose WPA-PSK or WPA2-PSK mode and access WPS again.

Below shows **Wireless LAN>>WPS** web page.

Wireless LAN >> WPS (Wi-Fi Protected Setup)

🗹 Enable WPS 🗘

Wi-Fi Protected Setup Information

WPS Status	Configured
SSID	DrayTek
Authentication Mode	Disable

Device Configure

Configure via Push Button	Start PBC
Configure via Client PinCode	Start PIN

Status: The Authentication Mode is NOT WPA/WPA2 PSK!!

Note: WPS can help your wireless client automatically connect to the Access point.

: WPS is Disabled.

🖸: WPS is Enabled.

arepsilon: Waiting for WPS requests from wireless clients.

Enable WPS	Check this box to enable WPS setting.
WPS Status	Display related system information for WPS. If the wireless security (encryption) function of the router is properly configured, you can see 'Configured' message here.
SSID	Display the SSID1 of the router. WPS is supported by SSID1 only.
Authentication Mode	Display current authentication mode of the router. Only WPA2/PSK and WPA/PSK support WPS.
Configure via Push Button	Click Start PBC to invoke Push-Button style WPS setup procedure. The router will wait for WPS requests from wireless clients about two minutes. The WPS LED on the router will blink fast when WPS is in progress. It will return to normal condition after two minutes. (You need to setup WPS within two minutes)
Configure via Client PinCode	Please input the PIN code specified in wireless client you wish to connect, and click Start PIN button. The WPS LED on the router will blink fast when WPS is in progress. It will return to normal condition after two minutes. (You need to setup WPS within two minutes)

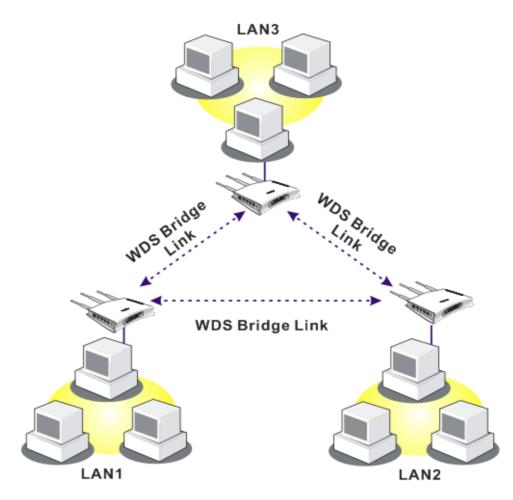
4.13.6 WDS

WDS means Wireless Distribution System. It is a protocol for connecting two access points (AP) wirelessly. Usually, it can be used for the following application:

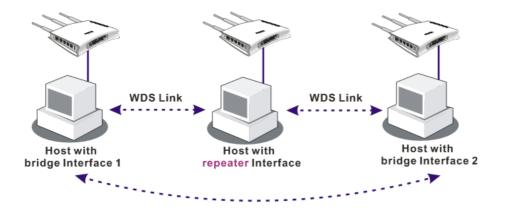
- Provide bridge traffic between two LANs through the air.
- Extend the coverage range of a WLAN.

To meet the above requirement, two WDS modes are implemented in Vigor router. One is **Bridge**, the other is **Repeater**. Below shows the function of WDS-bridge interface:





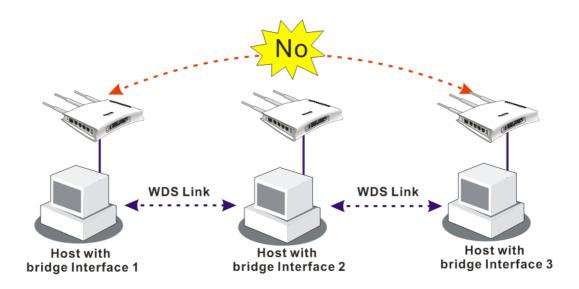
The application for the WDS-Repeater mode is depicted as below:



The major difference between these two modes is that: while in **Repeater** mode, the packets received from one peer AP can be repeated to another peer AP through WDS links. Yet in **Bridge** mode, packets received from a WDS link will only be forwarded to local wired or wireless hosts. In other words, only Repeater mode can do WDS-to-WDS packet forwarding.

In the following examples, hosts connected to Bridge 1 or 3 can communicate with hosts connected to Bridge 2 through WDS links. However, hosts connected to Bridge 1 CANNOT communicate with hosts connected to Bridge 3 through Bridge 2.





Click WDS from Wireless LAN menu. The following page will be shown.

Wireless LAN >> WDS Settings

Mode: Disable 🗸	Bridge
	Enable Peer MAC Address
Security:	
Disable OWEP Pre-shared Key	
WEP:	
Use the same WEP key set in <u>Security Settings</u> .	Note: Disable unused links to get better
	performance:
Pre-shared Key:	·
Туре:	Repeater
Interpreter DrayTek WPA OWPA OWPA2	Enable Peer MAC Addess
Key : *********	
Type 8~63 ASCII characters or 64 hexadecimal digits leading by "0x", for example "cfgs01a2" or	
"0x655abcd".	
	Access Point Function:
	Enable Disable
	Status:
	Send "Hello" message to peers.
	Link Status
	Note: The status is valid only when the peer also supports this function.



Choose the mode for WDS setting. **Disable** mode will not invoke any WDS setting. **Bridge** mode is designed to fulfill the

	first type of application. Repeater mode is for the second one. Disable Disable Bridge Repeater
Security	There are three types for security, Disable , WEP and Pre-shared key . The setting you choose here will make the following WEP or Pre-shared key field valid or not. Choose one of the types for the router.
WEP	Check this box to use the same key set in Security Settings page. If you did not set any key in Security Settings page, this check box will be dimmed.
Pre-shared Key	Type 8 ~ 63 ASCII characters or 64 hexadecimal digits leading by " $0x$ ".
Bridge	If you choose Bridge as the connecting mode, please type in the peer MAC address in these fields. Four peer MAC addresses are allowed to be entered in this page at one time. Yet please disable the unused link to get better performance. If you want to invoke the peer MAC address, remember to check Enable box in the front of the MAC address after typing.
Repeater	If you choose Repeater as the connecting mode, please type in the peer MAC address in these fields. Four peer MAC addresses are allowed to be entered in this page at one time. Similarly, if you want to invoke the peer MAC address, remember to check Enable box in the front of the MAC address after typing.
Access Point Function	Click Enable to make this router serving as an access point; click Disable to cancel this function.
Status	It allows user to send "hello" message to peers. Yet, it is valid only when the peer also supports this function.

4.13.7 Advanced Setting

This page allows users to set advanced settings such as operation mode, channel bandwidth, guard interval, and aggregation MSDU for wireless data transmission.

Wireless LAN >> Advanced Setting

Operation Mode	💿 Mixed Mode 🔘 Green Field	
Channel Bandwidth	O 20 💿 20/40	
Guard Interval	🔘 long 💿 auto	
Aggregation MSDU(A-MSDU)	🔘 Disable 💿 Enable	

Operation Mode

Mixed Mode – the router can transmit data with the ways supported in both 802.11a/b/g and 802.11n standards. However, the entire wireless transmission will be slowed down if 802.11g or 802.11b wireless client is connected. Green Field – to get the highest throughput, please choose such mode. Such mode can make the data transmission happening between 11n systems only. In addition, it does



	not have protection mechanism to avoid the conflict with neighboring devices of 802.11a/b/g.
Channel Bandwidth	 20- the router will use 20Mhz for data transmission and receiving between the AP and the stations. 20/40 – the router will use 20Mhz or 40Mhz for data transmission and receiving according to the station capability. Such channel can increase the performance for data transit.
Guard Interval	It is to assure the safety of propagation delays and reflections for the sensitive digital data. If you choose auto as guard interval, the AP router will choose short guard interval (increasing the wireless performance) or long guard interval for data transmit based on the station capability.
Aggregation MSDU	Aggregation MSDU can combine frames with different sizes. It is used for improving MAC layer's performance for some brand's clients. The default setting is Enable .

4.13.8 WMM Configuration

WMM is an abbreviation of Wi-Fi Multimedia. It defines the priority levels for four access categories derived from 802.1d (prioritization tabs). The categories are designed with specific types of traffic, voice, video, best effort and low priority data. There are four accessing categories - AC_BE, AC_BK, AC_VI and AC_VO for WMM.

APSD (automatic power-save delivery) is an enhancement over the power-save mechanisms supported by Wi-Fi networks. It allows devices to take more time in sleeping state and consume less power to improve the performance by minimizing transmission latency. Such function is designed for mobile and cordless phones that support VoIP mostly.

MM Capable	💿 Enable 🔘 Disable					
PSD Capable		🔘 Enable 💿 Disable				
VMM Parame	ters of Acc	ess Point				
	Aifsn	CWMin	CWMax	Тхор	ACM	AckPolicy
AC_BE	3	4	6	0		
АС_ВК	7	4	10	0		
AC_VI	1	3	4	94		
AC_VO	1	2	3	47		
VMM Parame	ters of Stat	ion				
	Aifsn	CWMi	in C	:WMax	Тхор	ACM
AC_BE	3	4	10)	0	
АС_ВК	7	4	10)	0	
AC_VI	2	3	4		94	
AC_VO	2	2	3		47	

Wireless LAN >> WMM Configuration

WMM Capable

To apply WMM parameters for wireless data transmission, please click the **Enable** radio button.



APSD Capable	The default setting is Disable .
Aifsn	It controls how long the client waits for each data transmission. Please specify the value ranging from 1 to 15. Such parameter will influence the time delay for WMM accessing categories. For the service of voice or video image, please set small value for AC_VI and AC_VO categories For the service of e-mail or web browsing, please set large value for AC_BE and AC_BK categories.
CWMin/CWMax	CWMin means contention Window-Min and CWMax means contention Window-Max. Please specify the value ranging from 1 to 15. Be aware that CWMax value must be greater than CWMin or equals to CWMin value. Both values will influence the time delay for WMM accessing categories. The difference between AC_VI and AC_VO categories must be smaller; however, the difference between AC_BE and AC_BK categories must be greater.
Тхор	It means transmission opportunity. For WMM categories of AC_VI and AC_VO that need higher priorities in data transmission, please set greater value for them to get highest transmission opportunity. Specify the value ranging from 0 to 65535.
ACM	It is an abbreviation of Admission control Mandatory. It can restrict stations from using specific category class if it is checked.
	Note: Vigor2110 provides standard WMM configuration in the web page. If you want to modify the parameters, please refer to the Wi-Fi WMM standard specification.
AckPolicy	"Uncheck" (default value) the box means the AP router will answer the response request while transmitting WMM packets through wireless connection. It can assure that the peer must receive the WMM packets. "Check" the box means the AP router will not answer any response request for the transmitting packets. It will have better performance with lower reliability.

Dray Tek

4.13.9 AP Discovery

Vigor router can scan all regulatory channels and find working APs in the neighborhood. Based on the scanning result, users will know which channel is clean for usage. Also, it can be used to facilitate finding an AP for a WDS link. Notice that during the scanning process (about 5 seconds), no client is allowed to connect to Vigor.

This page is used to scan the existence of the APs on the wireless LAN. Yet, only the AP which is in the same channel of this router can be found. Please click **Scan** to discover all the connected APs.

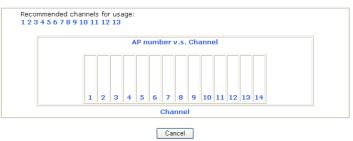


Access Point List				
	BSSID	Channel	SSID	
	r <u> </u>	Scan		1
See <u>St</u>	atistics.			
	Ouring the scanning pro t with the router.	cess (~5 seco	nds), no station is allowed to	
Add to	WDS Settings :			
AP's MA	.C address	:	: : : :	
Add t	to	💿 Bridge	○ Repeater	

Scan

It is used to discover all the connected AP. The results will be shown on the box above this button.





Add to

If you want the found AP applying the WDS settings, please type in the AP's MAC address on the bottom of the page and click Bridge or Repeater. Next, click **Add to**. Later, the MAC address of the AP will be added to Bridge or Repeater field of WDS settings page.

Dray Tek

4.13.10 Station List

Station List provides the knowledge of connecting wireless clients now along with its status code. There is a code summary below for explanation. For convenient **Access Control**, you can select a WLAN station and click **Add to Access Control** below.

	Status	MAC Address	Associated with
		Refresh	
	atus Codes :		
	Connected, I Connected, V	No encryption. NEP.	
	Connected, \ Connected, '		
B :	Blocked by A	ccess Control.	
	Connecting. Fail to pass V	VPA/PSK authentication.	
		tation connects to the rou ut notice. In that case, it	ter successfully, it may be will still be on the list until the
	onnection expi		
A	dd to <u>Access</u> (Control :	
Cli	ient's MAC ad	dress ::::	
		Add	
sh		Click this bu	itton to refresh the status of sta

Wireless LAN >> Station List

Add

Click this button to add current typed MAC address into Access Control.

4.14 System Maintenance

For the system setup, there are several items that you have to know the way of configuration: Status, Administrator Password, Configuration Backup, Syslog, Time setup, Reboot System, Firmware Upgrade.

Below shows the menu items for System Maintenance.



System Maintenance

- System Statu
- TR-069
- Administrator Password
- Configuration Backup
- SysLog / Mail Alert
- Time and Date
- Managemen
- Reboot System
- Firmware Upgrade

4.12.1 System Status

The **System Status** provides basic network settings of Vigor router. It includes LAN and WAN interface information. Also, you could get the current running firmware version or firmware related information from this presentation.

System Status

Model Name Firmware Version	: Vigor2110 series : 3.3.1		
Build Date/Time	: Jul 29 2009 17:05:31		
	LAN		WAN 1
MAC Address	: 00-50-7F-9A-32-70	Link Status	: Connected
1st IP Address	: 192.168.1.1	MAC Address	: 00-50-7F-9A-32-71
1st Subnet Mask	: 255.255.255.0	Connection	: DHCP Client
DHCP Server	: Yes	IP Address	: 192.168.5.29
DNS	: 168.95.1.1	Default Gateway	: 192.168.5.1
	VoIP	Wi	reless LAN
Port Prof	ile Reg. In/Out	MAC Address	: 00-50-7F-9A-32-70
Phone1	No 0/0	Frequency Domain	: Europe
Phone2	No 0/0	Firmware Version	: 1.8.1.0

SSID

: DrayTek

Model Name	Display the model name of the router.
Firmware Version	Display the firmware version of the router.
Build Date/Time	Display the date and time of the current firmware build.
ADSL Firmware Version	Display the ADSL firmware version.
LAN	
MAC Address	Display the MAC address of the LAN Interface.
1 st IP Address	Display the IP address of the LAN interface.
1 st Subnet Mask	Display the subnet mask address of the LAN interface.
DHCP Server	Display the current status of DHCP server of the LAN interface.
DNS	Display the assigned IP address of the primary DNS.
WAN	
Link Status	Display current connection status.
MAC Address	Display the MAC address of the WAN Interface.
Connection	Display the connection type.



IP Address	Display the IP address of the WAN interface.
Default Gateway	Display the assigned IP address of the default gateway.
Wireless LAN	
MAC Address	Display the MAC address of the wireless LAN.
Frequency Domain	It can be Europe (13 usable channels), USA (11 usable channels) etc. The available channels supported by the wireless products in different countries are various.
Firmware Version	It indicates information about equipped WLAN miniPCi card. This also helps to provide availability of some features that are bound with some WLAN miniPCi.
SSID	Display the SSID of the router.

4.14.2 TR-069

This device supports TR-069 standard. It is very convenient for an administrator to manage a TR-069 device through an Auto Configuration Server, e.g., VigorACS.

System Maintenance >> TR-069	Setting		
ACS and CPE Settings			
ACS Server On	Internet V		
ACS Server			
URL			
Username			
Password			
CPE Client			
🔘 Enable 💿 Disable			
URL			
Port	8069		
Username	vigor		
Password			
Periodic Inform Settings			
🔘 Disable			
💿 Enable			
Interval Time	900 second(s)		
	ОК		
CS Server On	Choose the interface for the router connecting to ACS server.		
CS Server	URL/Username/Password – Such data must be typed according to the ACS (Auto Configuration Server) y want to link. Please refer to Auto Configuration Server user's manual for detailed information.		
PE Client	It is not necessary for you to type them. Such informati is useful for Auto Configuration Server. Enable/Disable – Sometimes, port conflict might		



occurred. To solve such problem, you might want to

change port number for CPE. Please click Enable and change the port number.

Periodic Inform Settings

The default setting is **Enable**. Please set interval time or schedule time for the router to send notification to CPE. Or click **Disable** to close the mechanism of notification.

4.14.3 Administrator Password

This page allows you to set new password.

System Maintenance >> Administrator Password Setup

Administrator Password			
Old Password			
New Password			
Confirm Password			
Old Password	ок Type in the old password. The factory default setting for password is "admin" .		
New Password	Type in new password in this field.		
Confirm Password	Type in the new password again.		
When you click OK the login w	undow will appear. Plassa use the new password to access it		

When you click OK, the login window will appear. Please use the new password to access into the web configurator again.

Dray Tek

4.14.4 Configuration Backup

Backup the Configuration

Follow the steps below to backup your configuration.

1. Go to **System Maintenance** >> **Configuration Backup**. The following windows will be popped-up, as shown below.

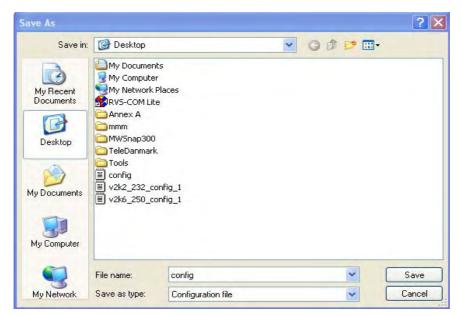
System Maintenance >> Configuration Backup			
Configuration	Backup / Restoration		
Restoration			
	Select a configuration file. Browse. Click Restore to upload the file. Restore		
Backup	Click Backup to download current running configurations as a file. Backup Cancel		

2. Click **Backup** button to get into the following dialog. Click **Save** button to open another dialog for saving configuration as a file.

File Dos	vnload 🔀
?	You are downloading the file: config.cfg from 192.168.1.1 Would you like to open the file or save it to your computer? Open Save Cancel More Info I Always ask before opening this type of file

3. In **Save As** dialog, the default filename is **config.cfg**. You could give it another name by yourself.





4. Click **Save** button, the configuration will download automatically to your computer as a file named **config.cfg**.

The above example is using **Windows** platform for demonstrating examples. The **Mac** or **Linux** platform will appear different windows, but the backup function is still available.

Note: Backup for Certification must be done independently. The Configuration Backup does not include information of Certificate.

Restore Configuration

1. Go to **System Maintenance** >> **Configuration Backup**. The following windows will be popped-up, as shown below.

System Maintenance >> Configuration Backup

Configuration	Backup / Restoration
Restoration	
	Select a configuration file.
	Browse.
	Click Restore to upload the file.
	Restore
Backup	
	Click Backup to download current running configurations as a file.
	Backup Cancel

- 2. Click **Browse** button to choose the correct configuration file for uploading to the router.
- 3. Click **Restore** button and wait for few seconds, the following picture will tell you that the restoration procedure is successful.



4.14.5 Syslog/Mail Alert

SysLog function is provided for users to monitor router. There is no bother to directly get into the Web Configurator of the router or borrow debug equipments.

SysLog / Mail Alert Setup	
SysLog Access Setup	Mail Alert Setup
🗹 Enable	Enable Send a test e-mail
Server IP Address	SMTP Server
Destination Port 514	Mail To
Enable syslog message:	Return-Path
🗹 Firewall Log	Authentication
VPN Log	User Name
🗹 User Access Log	Password
🗹 Call Log	Enable E-Mail Alert:
🗹 WAN Log	🗹 DoS Attack
Router/DSL information	M-P2P

Enable (Syslog Access)	Check "Enable" to activate function of syslog.
Syslog Server IP	The IP address of the Syslog server.
Destination Port	Assign a port for the Syslog protocol.
Enable syslog message	Check the box listed on this web page to send the corresponding message of firewall, VPN, User Access, Call, WAN, Router/DSL information to Syslog.
Enable (Alert Setup)	Check "Enable" to activate function of mail alert.
Send a test e-mail	Make a simple test for the e-mail address specified in this page. Please assign the mail address first and click this button to execute a test for verify the mail address is available or not.
SMTP Server	The IP address of the SMTP server.
Mail To	Assign a mail address for sending mails out.
Return-Path	Assign a path for receiving the mail from outside.
Authentication	Check this box to activate this function while using e-mail application.
User Name	Type the user name for authentication.
Password	Type the password for authentication.
Enable E-mail Alert	Check the box to send alert message to the e-mail box while the router detecting the item(s) you specify here.

Click **OK** to save these settings.

For viewing the Syslog, please do the following:

1. Just set your monitor PC's IP address in the field of Server IP Address



2. Install the Router Tools in the **Utility** within provided CD. After installation, click on the **Router Tools>>Syslog** from program menu.



3. From the Syslog screen, select the router you want to monitor. Be reminded that in **Network Information**, select the network adapter used to connect to the router. Otherwise, you won't succeed in retrieving information from the router.

Dray Tek Syslog Controls LAN Status TX Pac 169	kets	192.168.1.1 Vigor series RX Packets 1470	WAN Stal	us ateway IP (Fixed) WAN IP (Fixed)	TX Packets 0 RX Packets 0	TX Rate 0 RX Rate 0 0
On Line Routers	Mask	ess Log Call Log MAC	WAN Log Others Host Name: NIC Description:	vivian	t State	er - Packet Sc 💙
192.168.1.1	255.255.2	00-50-7F-54-6	NIC Information — MAC Address: IP Address: Subnet Mask:	00-11-D8-E4-58-CE 192.168.1.10 255.255.255.0	Default Geteway: DHCP Server: Lease Obtained:	192.168.1.1 192.168.1.1 Mon Jan 22
	Refresh	>	DNS Servers;	168.95.1.1	Lease Obtained:	01:28:23 2007 Thu Jan 25 01:28:23 2007
ADSL Status Mod	• 	State	Up Speed	Down Speed	SNR Margin	Loop Att

4.14.6 Time and Date

System Maintenance >> Time and Date

It allows you to specify where the time of the router should be inquired from.

Current System Time	2000 Jan 2 Sun 3 : 31 : 21	
Setup		
🔘 Use Browser Time		
💿 Use Internet Time Clie	ent	
Server IP Address		pool.ntp.org
Time Zone		(GMT) Greenwich Mean Time : Dublin 🛛 👻
Enable Daylight Saving		
Automatically Update 1	interval	30 min 💙

Current System Time

Click **Inquire Time** to get the current time.



Use Browser Time	Select this option to use the browser time from the remote administrator PC host as router's system time.
Use Internet Time	Select to inquire time information from Time Server on the Internet using assigned protocol.
Time Protocol	Select a time protocol.
Server IP Address	Type the IP address of the time server.
Time Zone	Select the time zone where the router is located.
Automatically Update Interval	Select a time interval for updating from the NTP server.
Click OK to save these settings.	

4.14.7 Management

This page allows you to manage the settings for access control, access list, port setup, and SMP setup. For example, as to management access control, the port number is used to send/receive SIP message for building a session. The default value is 5060 and this must match with the peer Registrar when making VoIP calls.

Mana	igement Setup					
Man	agement Access Co	ontrol	Management Port Setup			
🗹 A	llow management fro	m the Internet	💿 User Define Ports 🛛 Default Ports			
	FTP Server		Telnet Port	23 (Default: 23)		
•	HTTP Server		HTTP Port	80 (Default: 80)		
•	HTTPS Server		HTTPS Port	443 (Default: 443)		
	_		FTP Port	21 (Default: 21)		
□ SSH Server ✓ Disable PING from the Internet			SSH Port	22 (Default: 22)		
Access List			SNMP Setup			
List	IP	Subnet Mask	📃 Enable SNMP Agent			
1		*	Get Community	public		
2		~	Set Community	private		
3		~	Manager Host IP			
			Trap Community	public		
			Notification Host IP			
			Trap Timeout	10 seconds		
			ĸ			

Allow management from the Internet	Enable the checkbox to allow system administrators to login from the Internet. There are several servers provided by the system to allow you managing the router from Internet. Check the box(es) to specify.
Disable PING from the Internet	Check the checkbox to reject all PING packets from the Internet. For security issue, this function is enabled by default.
Access List	You could specify that the system administrator can only login from a specific host or network defined in the list. A maximum of three IPs/subnet masks is allowed. List IP - Indicate an IP address allowed to login to the router.





	Subnet Mask - Represent a subnet mask allowed to login to the router.
Default Ports	Check to use standard port numbers for the Telnet and HTTP servers.
User Defined Ports	Check to specify user-defined port numbers for the Telnet, HTTP and FTP servers.
Enable SNMP Agent	Check it to enable this function.
Get Community	Set the name for getting community by typing a proper character. The default setting is public.
Set Community	Set community by typing a proper name. The default setting is private.
Manager Host IP	Set one host as the manager to execute SNMP function. Please type in IP address to specify certain host.
Trap Community	Set trap community by typing a proper name. The default setting is public.
Notification Host IP	Set the IP address of the host that will receive the trap community.
Trap Timeout	The default setting is 10 seconds.

4.14.8 Reboot System

The Web Configurator may be used to restart your router. Click **Reboot System** from **System** Maintenance to open the following page.

System Maintenance >> Reboot System

Reboot Syster	m	
	Do you want to reboot your router ?	
	Osing current configuration	
	O Using factory default configuration	
	ОК	

If you want to reboot the router using the current configuration, check **Using current** configuration and click **OK**. To reset the router settings to default values, check **Using** factory default configuration and click **OK**. The router will take 5 seconds to reboot the system.

Note: When the system pops up Reboot System web page after you configure web settings, please click **OK** to reboot your router for ensuring normal operation and preventing unexpect errors of the router in the future.



4.14.9 Firmware Upgrade

Before upgrading your router firmware, you need to install the Router Tools. The **Firmware Upgrade Utility** is included in the tools. The following web page will guide you to upgrade firmware by using an example. Note that this example is running over Windows OS (Operating System).

Download the newest firmware from DrayTek's web site or FTP site. The DrayTek web site is www.draytek.com (or local DrayTek's web site) and FTP site is ftp.draytek.com.

Click **System Maintenance>> Firmware Upgrade** to launch the Firmware Upgrade Utility.

System Maintenance >> Firmware Upgrade

Web Firmware Upgrade					
	Select a firmware file.			Browse.	
	Click Upgrade to upload the file.	Upgrade		Diowse	

TFTP Firmware Upgrade from LAN

Current Firmware Version: 3.3.1
Firmware Upgrade Procedures:
 Click "OK" to start the TFTP server. Open the Firmware Upgrade Utility or other 3-party TFTP client software. Check that the firmware filename is correct. Click "Upgrade" on the Firmware Upgrade Utility to start the upgrade. After the upgrade is compelete, the TFTP server will automatically stop running.
Do you want to upgrade firmware ? OK

Click OK. The following screen will appear. Please execute the firmware upgrade utility first.

System Maintenance >> Firmware Upgrade

TFTP server is running. Please execute a Firmware Upgrade Utility software to upgrade router's firmware. This server will be closed by itself when the firmware upgrading finished.

For the detailed information about firmware update, please go to Chapter 5.



4.15 Diagnostics

Diagnostic Tools provide a useful way to **view** or **diagnose** the status of your Vigor router. Below shows the menu items for Diagnostics.

Diagnostics

4.15.1 Dial-out Trigger

Click **Diagnostics** and click **Dial-out Trigger** to open the web page. The internet connection (e.g., PPPoE) is triggered by a package sending from the source IP address.

Diagnostics >> Dial-out Trigger

out	Triggered Packet Header	<u>Refresh</u>
	HEX Format:	
	00 00 00 00 00 00 00 00 00 00 00 00 00	
	00 00 00 00 00 00 00 00-00 00 00 00 00 0	
	00 00 00 00 00 00 00-00 00 00 00 00 00 0	
	00 00 00 00 00 00 00 00 00 00 00 00 00	
	00 00 00 00 00 00 00 00 00 00 00 00 00	
	00 00 00 00 00 00 00 00-00 00 00 00 00 0	
	Decoded Format:	
	0.0.0.0 -> 0.0.0.0	
	Pr 0 len 0 (0)	

Decoded Format

It shows the source IP address (local), destination IP (remote) address, the protocol and length of the package.

Refresh

Click it to reload the page.



4.15.2 Routing Table

Click **Diagnostics** and click **Routing Table** to open the web page.

```
Diagnostics >> View Routing Table
```

```
Current Running Routing Table | Refresh |

Key: C - connected, S - static, R - RIP, * - default, ~ - private

S~ 192.168.10.0/ 255.255.255.0 via 192.168.1.2, LAN

C~ 192.168.1.0/ 255.255.255.0 is directly connected, LAN

S~ 211.100.88.0/ 255.255.255.0 via 192.168.1.3, LAN
```

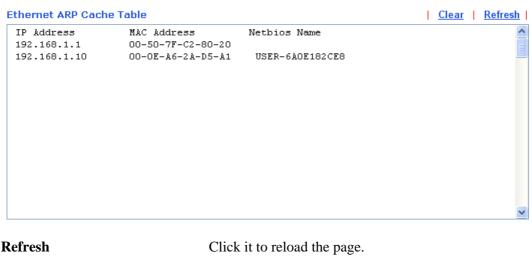
Refresh

Click it to reload the page.

4.15.3 ARP Cache Table

Click **Diagnostics** and click **ARP Cache Table** to view the content of the ARP (Address Resolution Protocol) cache held in the router. The table shows a mapping between an Ethernet hardware address (MAC Address) and an IP address.

```
Diagnostics >> View ARP Cache Table
```



Clear

Click it to clear the whole table.

4.15.4 DHCP Table

The facility provides information on IP address assignments. This information is helpful in diagnosing network problems, such as IP address conflicts, etc.

Click **Diagnostics** and click **DHCP Table** to open the web page.

```
Diagnostics >> View DHCP Assigned IP Addresses
```

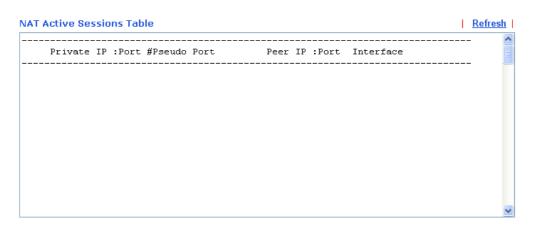
HCP se	rver: Running				
ndex		MAC Address	Leased Time	HOST ID	Ū

Index	It displays the connection item number.
IP Address	It displays the IP address assigned by this router for specified PC.
MAC Address	It displays the MAC address for the specified PC that DHCP assigned IP address for it.
Leased Time	It displays the leased time of the specified PC.
HOST ID	It displays the host ID name of the specified PC.
Refresh	Click it to reload the page.

4.15.5 NAT Sessions Table

Click **Diagnostics** and click **NAT Sessions Table** to open the list page.

Diagnostics >> NAT Sessions Table





Private IP:Port	It indicates the source IP address and port of local PC.
#Pseudo Port	It indicates the temporary port of the router used for NAT.
Peer IP:Port	It indicates the destination IP address and port of remote host.
Interface	It displays the representing number for different interface.
Refresh	Click it to reload the page.

4.15.6 Data Flow Monitor

Diagnostics >> Data Flow Monitor

This page displays the running procedure for the IP address monitored and refreshes the data in an interval of several seconds. The IP address listed here is configured in Bandwidth Management. You have to enable IP bandwidth limit and IP session limit before invoke Data Flow Monitor. If not, a notification dialog box will appear to remind you enabling it.

Click **Diagnostics** and click **Data Flow Monitor** to open the web page. You can click **IP** Address, TX rate, RX rate or Session link for arranging the data display.

	Refresh S	econds: 10 💌 Page: 1	*	<u>Refresh</u>
Index <u>IP Address</u>	<u>TX rate(Kbps)</u>	<u>RX rate(Kbps)</u> ↔	<u>Sessions</u>	Action
remaining time th	at the specified IP will be b	n in red, and the session	column will dis	play the
Enable Data Flow	at the specified IP will be t Check this box to			play the
remaining time th Enable Data Flow Monitor Refresh Seconds	Check this box to Use the drop dow	blocked.	me interval	of refresh
Enable Data Flow Monitor	Check this box to Use the drop dow	enable this function. n list to choose the ti done by the system at	me interval	of refresh
Enable Data Flow Aonitor Refresh Seconds	Check this box to Use the drop dow flow that will be Refresh Second	enable this function. n list to choose the ti done by the system at s: $10 \sim$ 10 15	me interval utomatically	of refresh
Enable Data Flow Aonitor	Check this box to Use the drop dow flow that will be o Refresh Second Click this link to	enable this function. n list to choose the ti done by the system at s: 10 10 15 30	me interval utomatically	of refresh

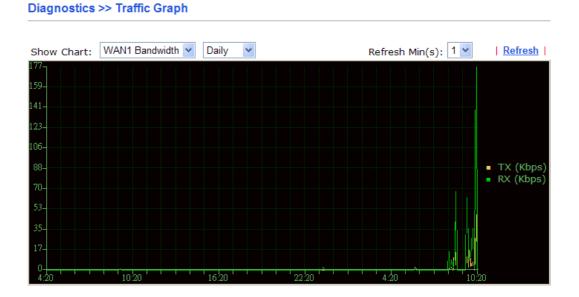
TX rate (kbps)	Display the transmission speed of the monitored device.		
RX rate (kbps)	Display the receiving speed of the monitored device.		
Sessions	Display the session number that you specified in Limit Session web page.		
Action	Block - can prevent specified PC accessing into Internet within 5 minutes.		
	age: 1 🛩 <u>Refresh</u>		
	os) 🗠 <u>Sessions</u> Action		
	7 Block		

Unblock – the device with the IP address will be blocked in five minutes. The remaining time will be shown on the session column.

age:	1 👻		<u>Refresh</u>
	5	essions	Action
	blo	cked / 298	<u>Unblock</u>

4.15.7 Traffic Graph

Click **Diagnostics** and click **Traffic Graph** to pen the web page. Choose WAN1 Bandwidth, Sessions, daily or weekly for viewing different traffic graph. Click **Refresh** to renew the graph at any time.



Dray Tek

4.15.8 Ping Diagnosis

Click **Diagnostics** and click **Ping Diagnosis** to pen the web page.

```
Diagnostics >> Ping Diagnosis
```

		g a LAN PC or you u gh, please select "Ur	on't want to specify nspecified".
Ping	to: Host / IP 🚩	IP Address:	
	Host / IP Gateway	Run	
Result	DNS		<u>Clear</u>
			~

Ping to	Use the drop down list to choose the destination that you want to ping.
IP Address	Type in the IP address of the Host/IP that you want to ping.
Run	Click this button to start the ping work. The result will be displayed on the screen.
Clear	Click this link to remove the result on the window.

4.15.9 Trace Route

Diagnostics >> Trace Route

Click **Diagnostics** and click **Trace Route** to open the web page. This page allows you to trace the routes from router to the host. Simply type the IP address of the host in the box and click **Run**. The result of route trace will be shown on the screen.

Trace Route			
Protocol:			
Host / IP	Address:	Run	
Result		1	<u>Clear</u>

Protocol

Use the drop down list to choose the interface that you want to ping through.

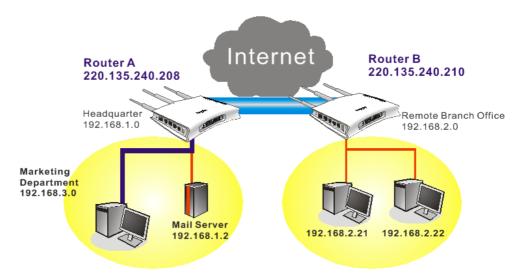
Host/IP Address	It indicates the IP address of the host.	
Run	Click this button to start route tracing work.	
Clear	Click this link to remove the result on the window.	

Dray Tek



5.1 Create a LAN-to-LAN Connection Between Remote Office and Headquarter

The most common case is that you may want to connect to network securely, such as the remote branch office and headquarter. According to the network structure as shown in the below illustration, you may follow the steps to create a LAN-to-LAN profile. These two networks (LANs) should NOT have the same network address.



Settings in Router A in headquarter:

VPN and Remote Access >> PPP General Setup

- 1. Go to **VPN and Remote Access** and select **Remote Access Control** to enable the necessary VPN service and click **OK**.
- 2. Then,

For using **PPP** based services, such as PPTP, L2TP, you have to set general settings in **PPP General Setup**.

rt IP Address 192.168.1.200

For using **IPSec**-based service, such as IPSec or L2TP with IPSec Policy, you have to set general settings in **IPSec General Setup**, such as the pre-shared key that both parties



have known.

VPN and Remote Access >> IPSec General Setup				
VPN IKE/IPSec General Setup		- 1.405		
Dial-in Set up for Remote Dial-in users IKE Authentication Method	and Dynamic IP Client (LAN t	O LAN).		
Pre-Shared Key	••••			
Confirm Pre-Shared Key	••••			
IPSec Security Method				
Medium (AH)				
Data will be authentic, but	will not be encrypted.			
	3DES 🔽 AES			
Data will be encrypted and	authentic.			
	OK Cancel			

- 3. Go to LAN-to-LAN. Click on one index number to edit a profile.
- 4. Set **Common Settings** as shown below. You should enable both of VPN connections because any one of the parties may start the VPN connection.

VPN and Remote Acc	ess >> LAN to LAN		
Profile Index : 1			
1. Common Settings			
Profile Name	Branch1	Call Direction 🤇 🧕	🖻 Both 🔘 Dial-Out 🔘 Dial-In
🔲 Enable this profile		🔲 Always on	
Netbios Naming Packet	💿 Pass i 🔘 Block	Idle Timeout	300 second(s)
		Enable PING to keep alive	
		PING to the IP	

5. Set **Dial-Out Settings** as shown below to dial to connect to Router B aggressively with the selected Dial-Out method.

If an *IPSec-based* service is selected, you should further specify the remote peer IP Address, IKE Authentication Method and IPSec Security Method for this Dial-Out connection.

Dray Tek

2. Dial-Out Settings

Type of Server I am calling PPTP IPSec Tunnel L2TP with IPSec Policy	Username ??? Password PPP Authentication PAP/CHAP V VJ Compression © On O Off
Server IP/Host Name for VPN. (such as draytek.com or 123.45.67.89) 220.135.240.210	IKE Authentication Method Pre-Shared Key IKE Pre-Shared Key Digital Signature(X.509) None IPSec Security Method Medium(AH) High(ESP) DES without Authentication Advanced Index(1-15) in <u>Schedule</u> Setup: , , , , ,

If a *PPP-based service* is selected, you should further specify the remote peer IP Address, Username, Password, PPP Authentication and VJ Compression for this Dial-Out connection.

Type of Server I am calling	Username	draytek		
● PPTP	Password	•••••		
IPSec Tunnel	PPP Authentication			
C L2TP with IPSec Policy None	VJ Compression	💿 On 🔘 Off		
Server IP/Host Name for VPN.	IKE Authentication M	ethod		
(such as draytek.com or 123.45.67.89)	Pre-Shared Key	Pre-Shared Key		
220.135.240.210	IKE Pre-Shared Key O Digital Signature(X.509)			
	None 🗸			
	IPSec Security Method Medium(AH)			
	O High(ESP) DES with	out Authentication 🎽		
	Advanced			
	Indeu(1, 15) in Selector	la Catura		
	Index(1-15) in <u>Schedu</u>	ie setup:		

6. Set **Dial-In settings** to as shown below to allow Router B dial-in to build VPN connection.

If an *IPSec-based* service is selected, you may further specify the remote peer IP Address, IKE Authentication Method and IPSec Security Method for this Dial-In connection. Otherwise, it will apply the settings defined in **IPSec General Setup** above.



3. Dial-In Settings

Allowed Dial-In Type		
PPTP	Username	???
🗹 IPSec Tunnel	Password	
L2TP with IPSec Policy None	VJ Compression	📀 On 🔘 Off
✓ Specify Remote VPN Gateway	IKE Authentication Meth	od
Peer VPN Server IP	✓ Pre-Shared Key	
220.135.240.210	IKE Pre-Shared Key	
or Peer ID	🔲 Digital Signature(X.509))
	None 👻	
	IPSec Security Method	
	Medium(AH)	
	High(ESP) 🛛 🗹 DES 🗹	3DES 🗹 AES

If a *PPP-based service* is selected, you should further specify the remote peer IP Address, Username, Password, and VJ Compression for this Dial-In connection.

3. Dial-In Settings		
Allowed Dial-In Type		
PPTP	Username	draytek
IPSec Tunnel	Password	•••••
L2TP with IPSec Policy None	VJ Compression	💿 On 🔘 Off
✓ Specify Remote VPN Gateway Peer VPN Server IP	IKE Authentication M	
220.135.240.210	IKE Pre-Shared Key	
	IPSec Security Meth	od
	Medium(AH)	
	High(ESP) 🗹 DES	3 🗹 3DES 🗹 AES

7. At last, set the remote network IP/subnet in **TCP/IP Network Settings** so that Router A can direct the packets destined to the remote network to Router B via the VPN connection.

4. TCP/IP Network Set	ings		
My WAN IP	0.0.0.0	RIP Direction	Disable 💌
Remote Gateway IP	0.0.0.0	From first subnet to remo	te network, you have to
Remote Network IP	192.168.2.0		Route 💌
Remote Network Mask	255.255.255.0		
	More	Change default route single WAN supports this	to this VPN tunnel (Only)
	ок с	lear Cancel	

Settings in Router B in the remote office:

- 1. Go to **VPN and Remote Access** and select **Remote Access Control** to enable the necessary VPN service and click **OK**.
- 2. Then, for using **PPP based** services, such as PPTP, L2TP, you have to set general settings in **PPP General Setup**.



VPN and Remote Access >> PPP General Setup

PPP/MP Protocol Dial-In PPP		IP Address Assignment for (When DHCP Disable set)	Dial-In Users
Authentication	PAP or CHAP 🔽	Start IP Address	192.168.2.200
Dial-In PPP Encryption (MPPE)	Optional MPPE		
Mutual Authentication	(PAP) (Yes 💿 No		
Username			
Password			

For using **IPSec-based** service, such as IPSec or L2TP with IPSec Policy, you have to set general settings in **IPSec General Setup**, such as the pre-shared key that both parties have known.

VPN and Remote Access >> IPSec General Setup

IKE Authentication Method		
Pre-Shared Key	••••	
Confirm Pre-Shared Key	••••	
IPSec Security Method		
🗹 Medium (AH)		
Data will be authentic, but	t will not be encrypted.	
High (ESP) 🛛 🗹 DES 📝	3DES 🗹 AES	
Data will be encrypted and	d authentic.	

- 3. Go to LAN-to-LAN. Click on one index number to edit a profile.
- 4. Set **Common Settings** as shown below. You should enable both of VPN connections because any one of the parties may start the VPN connection.

VPN and Remote Acce	ess >> LAN to LAN	
Profile Index : 1 1. Common Settings		
Profile Name	Branch1	Call Direction ③ Both 〇 Dial-Out 〇 Dial-In Always on
Netbios Naming Packet	⊙ Pass ○ Block	Idle Timeout 300 second(s) Enable PING to keep alive PING to the IP

5. Set **Dial-Out Settings** as shown below to dial to connect to Router B aggressively with the selected Dial-Out method.

If an *IPSec-based* service is selected, you should further specify the remote peer IP Address, IKE Authentication Method and IPSec Security Method for this Dial-Out connection.



2. Dial-Out Settings	
Type of Server I am calling	Username ???
О РРТР	Password
● IPSec Tunnel	PPP Authentication PAP/CHAP
O L2TP with IPSec Policy None	VJ Compression On Off
Server IP/Host Name for VPN.	IKE Authentication Method
(such as draytek.com or 123.45.67.89)	Pre-Shared Key
220.135.240.208	IKE Pre-Shared Key
	 Digital Signature(X.509)
	None 💌
	IPSec Security Method
	Medium(AH)
	O High(ESP) DES without Authentication
	Advanced
	Index(1-15) in <u>Schedule</u> Setup:

If a *PPP-based* service is selected, you should further specify the remote peer IP Address, Username, Password, PPP Authentication and VJ Compression for this Dial-Out connection.

2. Dial-Out Settings		
Type of Server I am calling	Username	draytek
• РРТР	Password	•••••
O IPSec Tunnel	PPP Authentication	
O L2TP with IPSec Policy None	VJ Compression	📀 On 🔘 Off
Server IP/Host Name for VPN.	IKE Authentication Meth	nod
(such as draytek.com or 123.45.67.89) 220.135.240.208	Pre-Shared Key	
220.135.240.206	IKE Pre-Shared Key	
	O Digital Signature(X.50	9)
	None 🗸	
	IPSec Security Method	
	Medium(AH)	
	O High(ESP) DES without	Authentication 👻
	Advanced	
	Index(1-15) in <u>Schedule</u>	Setup:
		,

6. Set **Dial-In settings** to as shown below to allow Router A dial-in to build VPN connection.

If an *IPSec-based* service is selected, you may further specify the remote peer IP Address, IKE Authentication Method and IPSec Security Method for this Dial-In connection. Otherwise, it will apply the settings defined in **IPSec General Setup** above.



3. Dial-In Settings

✓ Specify Remote VPN Gateway Peer VPN Server IP 220.135.240.208		
 PPTP ✓ IPSec Tunnel L2TP with IPSec Policy None ✓ Specify Remote VPN Gateway Peer VPN Server IP 220.135.240.208 IKE Auther Digital 		
□ L2TP with IPSec Policy None VJ Compre ☑ Specify Remote VPN Gateway IKE Auther Peer VPN Server IP IME Pre-Sha 220.135.240.208 Digital	ession 💿	
✓ Specify Remote VPN Gateway IKE Auther Peer VPN Server IP ✓ Pre-Sha 220.135.240.208 □ Digital	ession 💿 i	
✓ Specify Remote VPN Gateway Peer VPN Server IP 220.135.240.208		On 🔘 Off
None 🗸	re-Shared Key Signature(X.509) curity Method	S 🛛 AES

If a *PPP-based* service is selected, you should further specify the remote peer IP Address, Username, Password, and VJ Compression for this Dial-In connection.

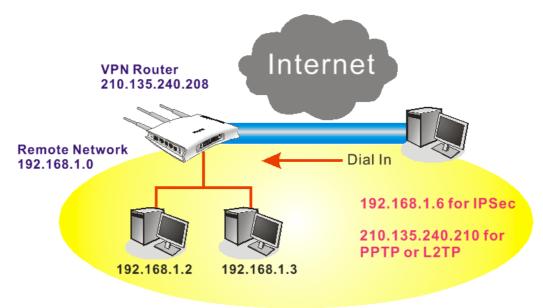
3. Dial-In Settings		
Allowed Dial-In Type		
🗹 РРТР	Username	draytek
🔲 IPSec Tunnel	Password	•••••
L2TP with IPSec Policy None	VJ Compression	💿 On 🔘 Off
Specify Remote VPN Gateway Peer VPN Server IP 220.135.240.208	IKE Authentication ✓ Pre-Shared Key IKE Pre-Shared Ke	
or Peer ID	Digital Signature(×.509)
	IPSec Security Met	nod
	🗹 Medium(AH)	
	High(ESP) 🗹 DES	6 🗹 3DES 🗹 AES

7. At last, set the remote network IP/subnet in **TCP/IP Network Settings** so that Router B can direct the packets destined to the remote network to Router A via the VPN connection.

4. TCP/IP Network Setti	ngs		
My WAN IP	0.0.0.0	RIP Direction	Disable 💌
Remote Gateway IP	0.0.0.0	From first subnet to remo do	te network, you have to
Remote Network IP	192.168.1.0		Route 💌
Remote Network Mask	255.255.255.0		
	More	Change default route single WAN supports this	
	ОК СІ	ear Cancel	

5.2 Create a Remote Dial-in User Connection Between the Teleworker and Headquarter

The other common case is that you, as a teleworker, may want to connect to the enterprise network securely. According to the network structure as shown in the below illustration, you may follow the steps to create a Remote User Profile and install Smart VPN Client on the remote host.



Settings in VPN Router in the enterprise office:

VPN and Remote Access >> PPP General Setup

- 1. Go to **VPN and Remote Access** and select **Remote Access Control** to enable the necessary VPN service and click **OK**.
- 2. Then, for using PPP based services, such as PPTP, L2TP, you have to set general settings in **PPP General Setup**.

PPP/MP Protocol		IP Address Assignme	nt for Dial-In Users
Dial-In PPP	PAP or CHAP	(When DHCP Disable s	set)
Authentication		Start IP Address	192.168.1.200
Dial-In PPP Encryption (MPPE)	Optional MPPE		
Mutual Authentication	(PAP) (Yes 💽 No		
Username			
Password			

For using IPSec-based service, such as IPSec or L2TP with IPSec Policy, you have to set general settings in **IKE/IPSec General Setup**, such as the pre-shared key that both parties have known.



VPN and Remote Access >> IPSec General Setup

VPN and Remote Access >> Remote Dial-in User

VPN IKE/IPSec General Setup

Dial-in Set up for Remote Dial-in users and [Dynamic IP Client (LAN to LAN).	
IKE Authentication Method		
Pre-Shared Key	•••••	
Confirm Pre-Shared Key	•••••	
IPSec Security Method		
🗹 Medium (AH)		
Data will be authentic, but will not be encrypted.		
High (ESP) ✓ DES	✓ AES entic	
Data will be encrypted and addin		
	OK Cancel	

- 3. Go to **Remote Dial-In User**. Click on one index number to edit a profile.
- 4. Set **Dial-In** settings to as shown below to allow the remote user dial-in to build VPN connection.

If an *IPSec-based* service is selected, you may further specify the remote peer IP Address, IKE Authentication Method and IPSec Security Method for this Dial-In connection. Otherwise, it will apply the settings defined in **IPSec General Setup** above.

User account and Authentication	Username ???
Enable this account dle Timeout 300 second(s)	Password
	IKE Authentication Method
Allowed Dial-In Type	🖉 Pre-Shared Key
PPTP	IKE Pre-Shared Key
🗹 IPSec Tunnel	Digital Signature(X.509)
🗌 L2TP with IPSec Policy None 💌	
🗌 Specify Remote Node	
Remote Client IP or Peer ISDN Number	IPSec Security Method
	Medium(AH)
or Peer ID	High(ESP) 🗹 DES 🗹 3DES 🗹 AES
Netbios Naming Packet 💿 Pass 🔘 Block	Local ID (optional)

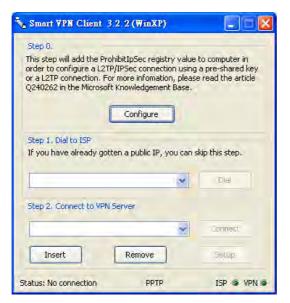
If a *PPP-based* service is selected, you should further specify the remote peer IP Address, Username, Password, and VJ Compression for this Dial-In connection.

VPN and Remote Access >> Remote Dial-in User

Index No. 1		
User account and Authentication	Username ???	
🔲 Enable this account	Password	
Idle Timeout 300 second(s)		
	IKE Authentication Method	
Allowed Dial-In Type	🗹 Pre-Shared Key	
✓ РРТР	IKE Pre-Shared Key	
🔲 IPSec Tunnel	Digital Signature(X.509)	
L2TP with IPSec Policy None	None V	
Specify Remote Node		
Remote Client IP or Peer ISDN Number	IPSec Security Method	
	Medium(AH)	
or Peer ID	High(ESP) 🗹 DES 🗹 3DES 🗹 AES	
Netbios Naming Packet Pass Block	Local ID (optional)	
OK Clear Cancel		

Settings in the remote host:

- 1. For Win98/ME, you may use "Dial-up Networking" to create the PPTP tunnel to Vigor router. For Win2000/XP, please use "Network and Dial-up connections" or "Smart VPN Client", complimentary software to help you create PPTP, L2TP, and L2TP over IPSec tunnel. You can find it in CD-ROM in the package or go to www.draytek.com download center. Install as instructed.
- 2. After successful installation, for the first time user, you should click on the **Step 0. Configure** button. Reboot the host.



3. In Step 2. Connect to VPN Server, click Insert button to add a new entry.

If an IPSec-based service is selected as shown below,



Session Name:	Office	
VPN Server IP/HO	ST Name(s	such as 123.45.67.89 or draytek.com)
192.168.1.1		
User Name :	die re	
Password :		i.e.
Type of VPN		
ОРРТР		O L2TP
O IPSec Tunn	nel	OL2TP over IPSec
PPTP Encryption No encrypt Require an	nom	
Maximum 1	trangth m	ner Vption
-	askoursu	on remote network

You may further specify the method you use to get IP, the security method, and authentication method. If the Pre-Shared Key is selected, it should be consistent with the one set in VPN router.

	-				
My IP :	172.16.3.10	0			~
Type of IPSec					
O Standard	IPSec Tunnel	-			
Remote	Subnet :	U.			
Remote	Subnet Mask :	-55	~55	:55	<u>U</u>
• Virture IP	Dray	Tek Virture	Inter	face	Y
💿 Obtai	in an IP address a	automatica	ally (DF	HCP ove	er IPSec
O Speci	fy an IP address				
IP A	ddress:	L.	160		200
Subr	net Mask:	40 m	100 100	-455	0
Security Metho	od				
O Medium(A	н) 🤇	High(ESF	2		
MØS		DES			*
Authority Meth	bod				
On in	d Key : *****				
Pre-share	on Authority				
 Pre-share Certificati 	on Authority.		-	T Diam	Mgerm
	on Additioncy.			Dru	

If a PPP-based service is selected, you should further specify the remote VPN server IP address, Username, Password, and encryption method. The User Name and Password should be consistent with the one set up in the VPN router. To use default gateway on remote network means that all the packets of remote host will be directed to VPN server then forwarded to Internet. This will make the remote host seem to be working in the enterprise network.



Session Name:	office			
VPN Server IP/HC	ST Name(s	uch as 123.45.67.89 or draytek.com)		
192.168.1.1				
User Name :	draytek	_user1		
Password :	****			
Type of VPN				
• PPTP		OL2TP		
O IPSec Tun	nel	OL2TP over IPSec		
PPTP Encryption No encryp Require en Maximum	tion heryption	cryption		
×				

4. Click **Connect** button to build connection. When the connection is successful, you will find a green light on the right down corner.

5.3 QoS Setting Example

Assume a teleworker sometimes works at home and takes care of children. When working time, he would use Vigor router at home to connect to the server in the headquarter office downtown via either HTTPS or VPN to check email and access internal database. Meanwhile, children may chat on Skype in the restroom.

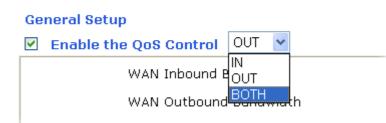
1. Go to Bandwidth Management>>Quality of Service.

Bandwidth Management >> Quality of Service

eneral	ootup							Factory D	oraan
Status	Bandwidth	Directon	Class 1	Class 2	Class 3	Others		ndwidth ntrol	
Enable	10000Kbps/10000Kbps	Outbound	25%	25%	25%	25%	Ina	ctive	Setup
Class Ru	le								
Class Ru Index		Name				Ru	ıle	Service ⁻	Type
	۲ <u>ــــــــــــــــــــــــــــــــــــ</u>	Name Test					ıle <u>lit</u>	Service ⁻	Туре
	< 1						lit	Service ⁻ <u>Edit</u>	

2. Click **Setup** link of WAN. Make sure the QoS Control on the left corner is checked. And select **BOTH** in **Direction**.

Bandwidth Management >> Quality of Service



3. Return to previous page. Enter the Name of Index Class 1 by clicking Edit link. Type the name "E-mail" for Class 1. Bandwidth Management >> Quality of Service

Class In	dex #1							
Name [E-mail							
NO	Status	Local Address	Remote Address	DiffServ CodePoint	Service Type			
1 🔿	Active	Any	Any	IP precedence 2	TFTP(UDP:69)			
	Add Edit Delete							
		٢	OK Cancel	7				

4. For this index, the user will set reserved bandwidth (e.g., 25%) for E-mail using protocol POP3 and SMTP.

General Setup				
Enable the	QoS Control BOTH 💌			
1	VAN Inbound Bandwidth	10000 Kbps		
v	VAN Outbound Bandwidth	10000 Kbps		
Index	Class Name	Reserved_bandwidth Ratio		
Class 1	E-mail	25 %		
Class 2		25 %		
Class 3		25 %		
	Others	25 <mark>%</mark>		
	Bandwidth Control CP ACK Prioritize	Limited_bandwidth Ratio 25 % Online Statistics		
	OK Clear	Cancel		

Bandwidth Management >> Quality of Service

Return to previous page. Enter the Name of Index Class 2 by clicking Edit link. In this index, the user will set reserved bandwidth for HTTPS. And click OK.
 Bandwidth Management >> Quality of Service

NO	Status				
	Status	Local Address	Remote Address	DiffServ CodePoint	Service Type
1 💿	Active	Any	Any	ANY	TFTP(UDP:69)
		4	Add Edit Delete]	

6. Click **Setup** link for WAN.

Bandwidth Management >> Quality of Service

Bandwidth Management >> Quality of Service

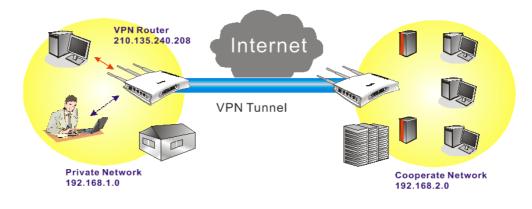
eneral	Setup						Set to Fact	ory Default
Status	Bandwidth	Directon	Class 1	Class 2	Class 3	Others	UDP Bandwi Control	
Enable	10000Kbps/10000Kbps	Both	25%	25%	25%	25%	Inactive	Setup
Place Dr	lo							
lass Ru Inde:		Name				Ru	ile Serv	vice Type
	۲ <u>ــــــــــــــــــــــــــــــــــــ</u>	Name E-mail				Ru <u>E</u> t		vice Type
	¢ 1						lit	vice Type <u>Edit</u>

7. Check **Enable UDP Bandwidth Control** on the bottom to prevent enormous UDP traffic of VoIP influent other application. Click **OK**.

General Setup		
Enable the	QoS Control BOTH 💌	
V	WAN Inbound Bandwidth	10000 Кыря
V	WAN Outbound Bandwidth	10000 Kbps
Index	Class Name	Reserved_bandwidth Ratio
Class 1	E-mail	25 %
Class 2	HTTPS	25 %
Class 3		25 %
	Others	25 <mark>%</mark>
	Bandwidth Control CP ACK Prioritize	Limited_bandwidth Ratio 25 % Online Statistics
	OK Clear	Cancel

8. If the worker has connected to the headquarter using host to host VPN tunnel. (Please refer to Chapter 3 VPN for detail instruction), he may set up an index for it. Enter the Class Name of Index 3. In this index, he will set reserved bandwidth for 1 VPN tunnel.





Bandwidth Management >> Quality of Service

lass Ind	ex #3				
ame V	'PN				
NO	Status	Local Address	Remote Address	DiffServ CodePoint	Service Type
1	Empty	-	-	-	-
			Add Edit Delet	е	
			OK Cancel		

9. Click Edit to open the following window. Check the ACT box, first.

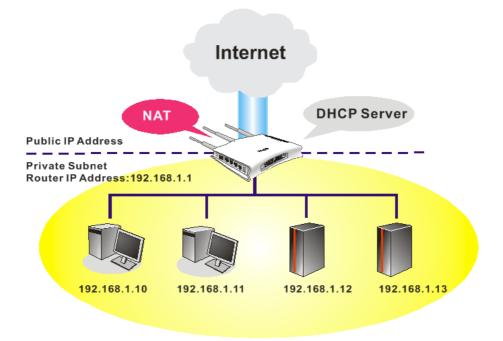
lit				
🗹 ACT				
Local Addres:	;	Any		E
Remote Addr	ess	Any		
DiffServ Code	Point	IP precedence 2	*	
Service Type		SYSLOG(UDP:514)	*	
Note: Please	choose/setup f	he <u>Service Type</u> first.		

10. Then click **Edit** of **Local Address** to set a worker's subnet address. Click **Edit** of **Remote Address** to set headquarter's IP address. Leave other fields and click **OK**.

5.4 LAN – Created by Using NAT

An example of default setting and the corresponding deployment are shown below. The default Vigor router private IP address/Subnet Mask is 192.168.1.1/255.255.255.0. The built-in DHCP server is enabled so it assigns every local NATed host an IP address of 192.168.1.x starting from 192.168.1.10.



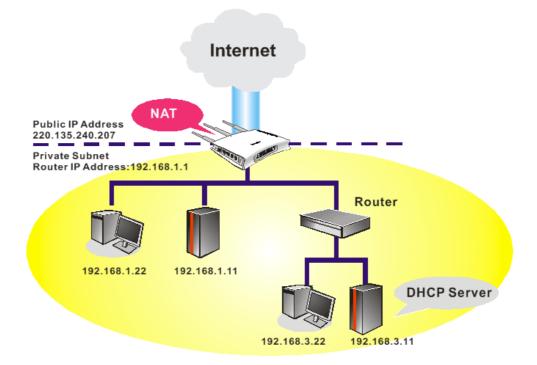


You can just set the settings wrapped inside the red rectangles to fit the request of NAT usage.

LAN >> General Setup

Ethernet TCP / IP and I	HCP Setup				
LAN IP Network Config	uration	DHCP Server Configuration			
For NAT Usage		⊙Enable Server ○Disable Server			
1st IP Address	192.168.1.5	Relay Agent: 🔿 1st Subnet 🔾 2nd Subnet			
1st Subnet Mask	255.255.255.0	Start IP Address	192.168.1.10		
For IP Routing Usage 🔘	Enable 💿 Disable	IP Pool Counts	50		
2nd IP Address	192.168.2.1	Gateway IP Address	192.168.1.5		
2nd Subnet Mask	255.255.255.0	DHCP Server IP Address			
2	nd Subnet DHCP Server	Tor Relay Agent			
		DNS Server IP Address			
RIP Protocol Control	Disable 💙	📃 Force DNS manual set	tting		
		Primary IP Address			
		Secondary IP Address			

To use another DHCP server in the network rather than the built-in one of Vigor Router, you have to change the settings as show below.



You can just set the settings wrapped inside the red rectangles to fit the request of NAT usage.

LAN >> General Setup

Ethernet TCP / IP and D	HCP Setup			
LAN IP Network Configu	Iration	DHCP Server Configurat	tion	
For NAT Usage		🔘 Enable Server 💿 Disab	ole Server	
1st IP Address	192.168.1.5	Relay Agent: 🔘 1st Subn	et 🔾 2nd Subnet	
1st Subnet Mask	255.255.255.0	Start IP Address	192.168.1.10	
For IP Routing Usage 🔘	Enable 💿 Disable	IP Pool Counts	50	
2nd IP Address	192.168.2.1	Gateway IP Address	192.168.1.5	
2nd Subnet Mask	255.255.255.0	DHCP Server IP Address	192.168.3.11	
2	nd Subnet DHCP Server	for Relay Agent		
		DNS Server IP Address		
RIP Protocol Control	Disable 👻	Force DNS manual setting		
		Primary IP Address		
		Secondary IP Address		
		Ж		

5.5 Calling Scenario for VoIP function

5.5.1 Calling via SIP Sever

Example 1: Both John and David have SIP Addresses from different service providers.

VolP >> DialPlan Setup

Phone Book Index No. 1

John's SIP URL: 1234@draytel.org, David's SIP URL: 4321@iptel.org

Settings for John

DialPlan index 1 Phone Number: 1111 Display Name: David SIP URL: 4321@iptel.org

SIP Accounts Settings ---

Profile Name: draytel1 Register via: Auto SIP Port: 5060 (default) Domain/Realm: draytel.org Proxy: draytel.org Act as outbound proxy: unhecked Display Name: John Account Number/Name: 1234 Authentication ID: unchecked Password: **** Expiry Time: (use default value)

	Phone Number	1111		
	Display Name	David		
	SIP URL	4321	p liptel org	
	Dial Out Account	Default 😁		
	Loop through	None 💌		
	Backup Phone Num	ber		
		OK Clear	Cancel	
oIP >> SIP Acc	counts			
OIP >> SIP Acc SIP Account Ind Profile	ex No. 1	draytel 1	11 char max.)	

Profile Name	draytel 1	(11 char ma:	x.)
Register	Auto 💌 🗌 Call wit	thout Registrat	ion
SIP Port	5060		
Domain/Realm	draytel.org		(63 char max.)
Proxy	draytel.org		(63 char max.)
Act as outbound pro	αy		
Display Name	Jahn	(23 char mai	x.)
Account Number/Name	1234		(63 char max.)
I Authentication ID			(63 char max.)
Password			(63 char max.)
Expiry Time	1 hour 💉 3600	sec	
NAT Traversal Support	None 👻		
Ring Port	Phone 1 Phone :	2	
Ring Pattern	1 ~		

John calls David ---

VolP >> DialPlan Setup

Enable

e Book Index No. 1

Phone Number

Display Name

Loop through

Dial Out Account

Backup Phone Numb

SIP URL

He picks up the phone and dials 1111#. (DialPlan Phone Number for David)

John

1234

Default

None 💌

OK Clear Cancel

@ draytel.org

Settings for David

(Use default value)

DialPlan index 1 Phone Number:2222 Display Name: John SIP URL:1234@draytel.org

CODEC/RTP/DTMF ---

SIP Accounts Settings ----

Profile Name: iptel 1 Register via: Auto SIP Port: 5060(default) Domain/Realm: iptel.org Proxy: iptel.org Act as outbound proxy: unchecked Display Name: David Account Name: 4321 Authentication ID: unchecked Password: **** Expiry Time: (use default value)

VoIP >> SIP Accounts SIP Account Index No. 1 iptel 1 Profile Name (11 char max.) Auto 🖌 Register Call without Registration 5060 SIP Port Domain/Realm iptel.org (63 char max.) Proxy (63 char max.) iptel.org Act as outbound **Display Name** (23 char max.) David Account Number/Name 4321 (63 char max.) Authentication ID (63 char max.) Password (63 char max.) Expiry Time 1 hour 😁 3600 sec NAT Traversal Su None 💌 Phone 1 Phone 2 Ring Port 1 ~ Ring Patter

CODEC/RTP/DTMF ----

David calls John

He picks up the phone and dials 2222# (DialPlan

OK Cancel



(Use default value)

Phone Number for John)

Example 2: Both John and David have SIP Addresses from the same service provider.

John's SIP URL: 1234@draytel.org , David's SIP URL: 4321@draytel.org

Settings for John DialPlan index 1 Phone Number: 1111 Display Name: David SIP URL: 4321@draytel.org

SIP Accounts Settings ----

Profile Name: draytel 1 Register via: Auto SIP Port: 5060 (default) Domain/Realm: draytel.org Proxy: draytel.org Act as outbound proxy: unchecked Display Name: John Account Number/Name: 1234 Authentication ID: unchecked Password: **** Expiry Time: (use default value)

CODEC/RTP/DTMF ---

(Use default value)

Settings for David

DialPlan index 1 Phone Number:2222 Display Name: John SIP URL:1234@draytel.org

SIP Accounts Settings ----

Profile Name: John Register via: Auto SIP Port: 5060(default) Domain/Realm: draytel.org Proxy: iptel.org Act as outbound proxy: unchecked Display Name: David Account Name: 4321 Authentication ID: unchecked Password: **** Expiry Time: (use default value)

CODEC/RTP/DTMF---

(Use default value)

Enable	Phone Number	1111	1	
	Display Name	David	-	
	SIP URL	4321	0	draytel.org
	Dial Out Account	Default 💌		And the second of the second se
	Loop through	None 😁		
	Backup Phone Number			
	OK	Clear	Cano	

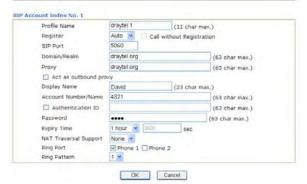
Profile Name	draytel 1	(11 char m	lax.)
Register	Auto 🎽 🗌 Call	ation	
SIP Port	5060		
Domain/Realm	draytel.org	(63 char max.)	
Proxy	draytel.org		(63 char max.)
Act as outbound pro	×y		
Display Name	John	(23 char m	ax.)
Account Number/Name	1234		(63 char max.)
Authentication ID			(63 char max.)
Password			(63 char max.)
Expiry Time	1 hour 😁 🔤	sec	
NAT Traversal Support	None 🛩		
Ring Port	Phone 1 Phone	ne 2	
Ring Pattern	1 *		

John calls David

He picks up the phone and dials 1111#. (DialPlan Phone Number for David) Or, He picks up the phone and dials 4321#. (David's Account Name)

Phone Book	Index No. 1		
Enable			
	Phone Number	2222	
	Display Name	John	
	SIP URL	1234	m draytel.org
	Dial Out Account	Default 😁	
	Loop through	None 😒	
	Backup Phone Number		

VoIP >> SIP Acco	unts	
------------------	------	--



David calls John

He picks up the phone and dials 2222# (DialPlan Phone Number for John) Or, He picks up the phone and dials 1234# (John's Account Name)



5.5.2 Peer-to-Peer Calling

Example 3: Arnor and Paulin have Vigor routers respectively. They can call each other *without* SIP Registrar. First they must have each other's IP address and assign an Account Name for the port used for calling.

Arnor's SIP URL: 1234@214.61.172.53

Settings for Arnor

DialPlan index 1 Phone Number: 1111 Display Name: paulin SIP URL: 4321@ 203.69.175.24

SIP Accounts Settings ---

Profile Name: Paulin Register via: None SIP Port: 5060(default) Domain/Realm: (blank) Proxy: (blank) Act as outbound proxy: unchecked Display Name: Arnor Account Name: 1234 Authentication ID: unchecked Password: (blank) Expiry Time: (use default value)

CODEC/RTP/DTMF---

(Use default value)

Settings for Paulin

DialPlan index 1 Phone Number:2222 Display Name: Arnor SIP URL: 1234@214.61.172.53

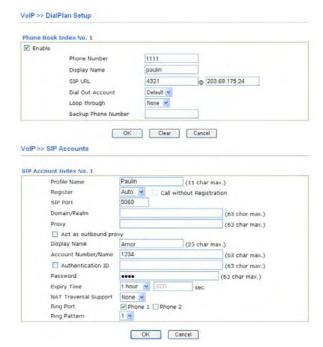
SIP Accounts Settings ----

Profile Name: Arnor Register via: None SIP Port: 5060(default) Domain/Realm: (blank) Proxy: (blank) Act as outbound proxy: unchecked Display Name: Paulin Acco4unt Name: 4321 Authentication ID: unchecked Password: (blank) Expiry Time: (use default value)

CODEC/RTP/DTMF---

(Use default value)

Paulin's SIP URL: 4321@ 203.69.175.24



Arnor calls Paulin

VolP >> SIP Accounts

He picks up the phone and dials **1111#**. (DialPlan Phone Number for Arnor)

Phone Book	Index No. 1		
🗹 Enable			
	Phone Number	2222	
	Display Name	Amor	
	SIP UPL	1234	@ 214.61.172.53
	Dial Out Account	Default 💌	
	Loop through	None 😁	
	Backup Phone Number		

rofile Name	Amor	(11 char	max.)
Register	Auto 🖌 🗌 Ca	Il without Regis	tration
SIP Port	5060		
Domain/Realm			(63 char max.)
Proxy			(63 char max.)
Act as outbound pro	xy		
Display Name	Paulin	(23 char	max.)
Account Number/Name	4321		(63 char max.)
Authentication ID			(63 char max.)
Password			(63 char max.)
Expiry Time	1 hour M 3600	sec	
NAT Traversal Support	None 🐱		
Ring Port	Phone 1 Pho	one 2	
Ring Pattern	1 ~		

Paulin calls Arnor

He picks up the phone and dials **2222**# (DialPlan Phone Number for John)



5.6 Upgrade Firmware for Your Router

Before upgrading your router firmware, you need to install the Router Tools. The **Firmware Upgrade Utility** is included in the tools.

- 1. Go to www.draytek.com.
- 2. Access into **Support** >> **Downloads**. Please find out **Firmware** menu and click it. Search the model you have and click on it to download the newly update firmware for your router.

	About DrayTek	Products Support	Education	Partners Contact L
ome > Support > Downloads	3			
Downloads - Firmware				Downloads
Model Name	Firmware Version	Release Date		Firmware
Vigor120 series	3.2.2.1	26/06/2009		Driver
Vigor2100 series	2.6.2	26/02/2008		Utility
Vigor2104 series	2.5.7.3	13/02/2008		Utility Introduction
Vigor2110 series	3.3.0	25/06/2009		Datasheet
Vigor2200/X/W/E	2.3.11	22/09/2004		R&TTE Certification
Vigor2200Eplus	2.5.7	18/02/2009		
Vigor2200USB	2.3.10	16/03/2005		

3. Access into **Support >> Downloads**. Please find out **Utility** menu and click it.

		About	DrayTek Products	Support Educati	on Partners Contact Us
ome > Support > Ut	ility				
Jtility					Downloads
Tools Name	Release Date	Version	os	Support Model	Firmware
Router Tools	2009/06/18	4.2.0	MS-Windows	All Modules	- Driver
Syslog Tools	2009/06/18	4.2.0	MS-Windows XP	All Modules	Driver
-,;			MS-Vista		Utility
VigorPro Alert Notice	2009/06/03	1.1.0	MS-Windows XP	VigorPro 100 series	Utility Introduction
Tools		(Multi- language)	MS-Vista	VigorPro 5500 series VigorPro 5510 series	Datasheet
				VigorPro 5300 series	R&TTE Certification
Smart VPN Client	2009/05/25	3.6.3	MS-Windows XP	All Modules	
		(Multi- language)	MS-Vista		
Smart Monitor	2009/03/25	2.0	MS-Windows XP	Vigor2950 series	-
				VigorPro 5510 series	

4. Click on the link of **Router Tools** to download the file. After downloading the files, please decompressed the file onto your host.

5. Double click on the icon of router tool. The setup wizard will appear.



- 6. Follow the onscreen instructions to install the tool. Finally, click **Finish** to end the installation.
- 7. From the Start menu, open Programs and choose Router Tools XXX >> Firmware Upgrade Utility.

៉ Firmware Upgrade	Utility 3.5.1	
Time Out(Sec.) 5	Router IP:	
Port	Firmware file:	
69		
Password:	Abort	Send

- 8. Type in your router IP, usually **192.168.1.1**.
- 9. Click the button to the right side of Firmware file typing box. Locate the files that you download from the company web sites. You will find out two files with different extension names, **xxxx.all** (keep the old custom settings) and **xxxx.rst** (reset all the custom settings to default settings). Choose any one of them that you need.

🐴 Firmware Upgrade	Utility 3.5.1
Time Out(Sec.) 5	Router IP:
Port	Firmware file:
69	C:\Documents and Settings\Carrie
Password:	Abort Send

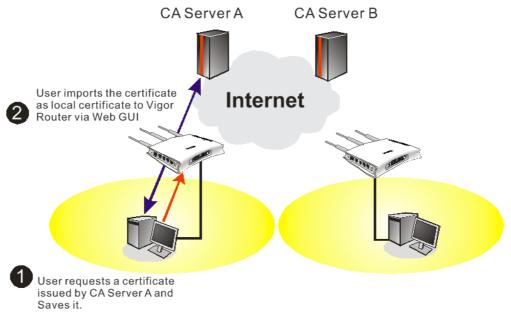


10. Click Send.

៉ Firmware Upgrade	Utility 3.5.1
Time Out(Sec.) 5	Router IP:
Port	Firmware file:
69	C:\Documents and Settings\Carrie
Password:	Abort Send
Sending	

11. Now the firmware update is finished.

5.7 Request a certificate from a CA server on Windows CA Server



1. Go to **Certificate Management** and choose **Local Certificate**.

Certificate Management >> Local Certificate

K509 Local Certificate Configuration				
Name	Subject	Status	Modify	
Local			View Delete	
GENERATE	IMPORT REFRESH			
X509 Loca	l Certificate			
			~	
			~	

2. You can click **GENERATE** button to start to edit a certificate request. Enter the information in the certificate request.

Certificate Management >> Local Certificate

Generate Certificate Request		
Subject Alternative Name		
Туре	IP Address 🛛 👻	
IP		
Subject Name		
Country (C)		
State (ST)		
Location (L)		
Orginization (O)		
Orginization Unit (OU)		
Common Name (CN)		
Email (E)		
Кеу Туре	RSA 🗸	
Key Size	1024 Bit 🔽	
	Generate	

3. Copy and save the X509 Local Certificate Requet as a text file and save it for later use. Certificate Management >> Local Certificate

X509 Local Cert	tificate Configuration				
Name	Subject Status Modify				
Local	/C=TW/ST=HC/L=HC/O=Draytek/O Requesting View Delete				
GENERATE	GENERATE IMPORT REFRESH				
X509 Lo	ocal Certificate				
MIIBqj EwJIQz CQEWE3 AoGBAL a1X//f m6+0f4 hkiG9w 9yojHp eorpDa	EGIN CERTIFICATE REQUEST CCARMCAQAwajELMAkGA1UEBhMCVFcxCzAJ EQMA4GA1UEChMHRHJheXR1azELMAkGA1UE N1cHBvcnRAZHJheXR1ay5jb20wg28wDQVJ MJdTsqfF97FEpYy+IqeJVJGuSRtqG6Etw6 gnEccQA2LPSQIQ85Qychwq07Bm0EDf10wF xZ4QQnjXXgciCOBj1iAa6MLSce1synZhkq OBAQUFAA0BgQCq3sdwVc21t9qn4U6X2BJs stNsmWsMRu&wGeKCWc8S/gLtHhr6iccMo7 1/rC92wCra0t8XUmPqNoiytq8DxStTE8VU ND CERTIFICATE REQUEST	CxMCUkQxIjAgE KoZIhvCNAQEBE yTUSHQvXpAzcr wCalAZQoGvIiC mQ1QN5uFAgMBA Vzu7JHafSSeUr 'oQFx/LWdaEPU5	gkqhkiG9w0B QADgYOAMIGJ GJBGrikTUBX DMC7f5w9xA8 LAGgADANBgkq LAYD2sfCmCfX SLqryBKKgC9t		

4. Connect to CA server via web browser. Follow the instruction to submit the request. Below we take a Windows 2000 CA server for example. Select **Request a Certificate**.

Welcome	
will be able to sec	ite to request a certificate for your web browser, e-mail client, or other secure program. Once you acquire a certificate, y urely identify yourself to other people over the web, sign your e-mail messages, encrypt your e-mail messages, and mor ne type of certificate you request.
Select a task:	
 Retrieve the Request a c 	CA certificate or certificate revocation list ertificate
-	pending certificate

Select Advanced request.

Microsoft Certificate Services vigor	Home
Choose Request Type	
Please select the type of request you would like to make:	
User certificate request. User Certificate	
Advanced request	
Next :	>

Select Submit a certificate request a base64 encoded PKCS #10 file or a renewal request using a base64 encoded PKCS #7 file

Microsoft Certificate Services vigor	Home
Advanced Certificate Requests	
You can request a certificate for yourself, another user, or a computer using one of the following m authority (CA) will determine the certificates that you can obtain.	nethods. Note that the policy of the certification
 Submit a certificate request to this CA using a form. 	
 Submit a certificate request using a base64 encoded PKCS #10 file or a renewal request using 	ing a base64 encoded PKCS #7 file.
 Request a certificate for a smart card on behalf of another user using the Smart Card Enrollm You must have an enrollment agent certificate to submit a request for another user. 	nent Station.
	Next >
mport the X509 Local Certificate Requet text file. Select 1	Router (Offline request) of
PSec (Offline request) below.	
Mierosoff Catillicata Saviega - viner	Hom

Submit A Save	The second second second		
		quest or PKCS #7 renewal request generated by an external application (such as a w o the certification authority (CA).	veb
	Charles have been been	a na compositives sum carbo	
Saved Request:			
Certificate Request (PKCS #10 or #7):	BEGIN CERTIFICATE REQU HIIBqjCCARMCAQAwQTELMAKGAIL BgkqhkiGSwDBCQEWEXByZXNQQG A4GNADCB1QKBgQDQYB7wmZFfFhh hX4bpB9cUF9dloACG61M/tcBock x/GOATCTvO/fQ2pxroCw1J1jL5	hMCVFcxEDAO X10ZMsuY29t I@QnG03Xk++ ZdFFr4IXcF3	
	Browse for a file to insert.		
Certificate Templa	ito.		
ceruncate rempia	Administrator		
Additional Attribut	Administrator Authenticated Session Basic EFS		
Attributes:	EFS Recovery Agent User IPSEC (Offline request)		
	Router (Offline request) Subordinate Certification Authority Web Server	Subm	nit >]

Then you have done the request and the server now issues you a certificate. Select **Base 64 encoded** certificate and **Download CA certificate**. Now you should get a certificate (.cer file) and save it.

5. Back to Vigor router, go to **Local Certificate**. Click **IMPORT** button and browse the file to import the certificate (.cer file) into Vigor router. When finished, click refresh and

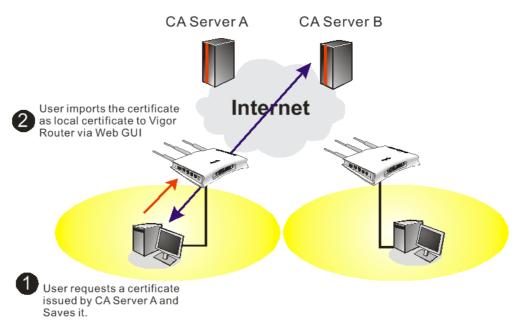
you will find the below window showing "-----BEGINE CERTIFICATE-----" Certificate Management >> Local Certificate

lame	e Subject Status Modify			
Local	/C=TW/ST=HC/L=HC/O=Draytek/O Requesting View		View Delete	
GENERATE IMPORT REFRESH				
X509 Lo	ocal Certificate			
MIIBqj EwJIQz CQEWE3 AoGBAL a1X//f m6+0f4 hkiG9w	EGIN CERTIFICATE REQUEST CCARMCAQAwajELMAkGA1UEBhMCVFcxCzAJ EQMA4GA1UEChMHRHJheXR1azELMAkGA1UE N1cHBvcnRA2HJheXR1ay5jb20wg28wDQVJ MJdTsqfF97FEpYy+IqeJVJGuSRtqG6EtwE gnEccQA2LPSQIQ85Qychwq07Bm0EDf10wE x24QQnjXXgciCOBj1iAa6MLScelsynZhkg OBAQUFAAOBgQCq3sdwVc21t9qn4U6X2BJs stNsmW3MRuàwGeKCWc8S/qLtHnr6iccMo7	CxMCUkQxIjAgH KoZIhvcNAQEBH YTUSHQvXpAzcr WCalAZQoGvIi (mQ1QNSuFAgMBJ Vzu7JHafSSeUh	SgkqhkiG9w0B SQADgYOAMIGJ SgJBGrikTUBX DDMC7f5w9xA8 AAGgADANBgkq haYDZefCmGfX	

6. You may review the detail information of the certificate by clicking **View** button.

Name :	Local
Issuer :	/C=US/CN=vigor
Subject :	/emailAddress=press@draytek.com/C=TV//O=Draytek
Subject Alternative Name :	DNS:draytek.com
Valid From :	Aug 30 23:08:43 2005 GMT
Valid To :	Aug 30 23:17:47 2007 GMT

5.8 Request a CA Certificate and Set as Trusted on Windows CA Server



1. Use web browser connecting to the CA server that you would like to retrieve its CA certificate. Click **Retrive the CA certificate or certificate recoring list**.



- 2. In Choose file to download, click CA Certificate Current and Base 64 encoded, and Download CA certificate to save the .cer. file.
 - Microsoft Certificate Services Microsoft Internet Explored 檔案(P) 編輯(E) 檢視(V) 我的最愛(A) 工具(I) 說明(H) 🌀 L-頁 • 🜍 - 📝 😰 🚮 🔎 搜尋 ☆ 我的最爱 🔮 媒體 🚱 🍰 漫 • 🥸 網址(D) 截 http://172.16.2.179/certsrv/certcarc.asp 🖌 🛃 移至 🧕 連結 msn. -💉 🔎 搜尋 • 🛃 醒目提示 🛃 選項 封鎖快顯視窗 (319) 🔹 🔤 Hotmail 🚢 Messenger [我的 MSN Retrieve The CA Certificate Or Certificate Revocation List Install this CA certification path to allow your computer to trust certificates issued from this certification authority. It is not necessary to manually install the CA certification path if you request and install a certificate from this certification authority, because the CA certification path will be installed for you automatically. Choose file to download: CA Certificate: Current (vigor(1)) Previous [vigor] Download CA certificate Download CA certification path Download latest certificate revocation list
- 3. Back to Vigor router, go to **Trusted CA Certificate**. Click **IMPORT** button and browse the file to import the certificate (.cer file) into Vigor router. When finished, click refresh and you will find the below illustration.

Certificate Management >> Trusted CA Certificate

X509 Trusted CA Certificate Configuration Name Subject Status Modify /C=US/CN=vigor Delete Trusted CA-1 View Not Yet Valid Trusted CA-2 ___ View Delete ___ View Delete Trusted CA-3 ___

REFRESH

4. You may review the detail information of the certificate by clicking **View** button.

IMPORT

Name :	Trusted CA-1
Issuer :	/C=US/CN=vigor
Subject :	/C=US/CN=vigor
Subject Alternative Name :	DNS:draytek.com
Valid From :	Aug 30 23:08:43 2005 GMT
Valid To :	Aug 30 23:17:47 2007 GMT

Close

Note: Before setting certificate configuration, please go to System Maintenance >> Time and Date to reset current time of the router first.

6 Trouble Shooting

This section will guide you to solve abnormal situations if you cannot access into the Internet after installing the router and finishing the web configuration. Please follow sections below to check your basic installation status stage by stage.

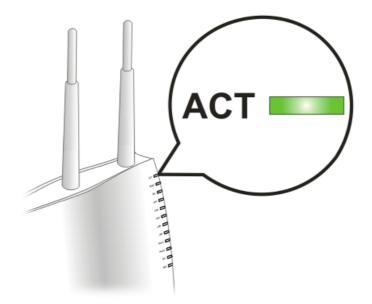
- Checking if the hardware status is OK or not.
- Checking if the network connection settings on your computer are OK or not.
- Pinging the router from your computer.
- Checking if the ISP settings are OK or not.
- Backing to factory default setting if necessary.

If all above stages are done and the router still cannot run normally, it is the time for you to contact your dealer for advanced help.

6.1 Checking If the Hardware Status Is OK or Not

Follow the steps below to verify the hardware status.

- 1. Check the power line and WLAN/LAN cable connections. Refer to "**1.3 Hardware Installation**" for details.
- 2. Turn on the router. Make sure the **ACT LED** blink once per second and the correspondent **LAN LED** is bright.



3. If not, it means that there is something wrong with the hardware status. Simply back to "**1.3 Hardware Installation**" to execute the hardware installation again. And then, try again.



6.2 Checking If the Network Connection Settings on Your Computer Is OK or Not

Sometimes the link failure occurs due to the wrong network connection settings. After trying the above section, if the link is stilled failed, please do the steps listed below to make sure the network connection settings is OK.

For Windows



The example is based on Windows XP. As to the examples for other operation systems, please refer to the similar steps or find support notes in **www.draytek.com**.

1. Go to **Control Panel** and then double-click on **Network Connections**.



2. Right-click on Local Area Connection and click on Properties.



3. Select Internet Protocol (TCP/IP) and then click Properties.

ieneral	Authentication Advanced
Connec	st using:
##	ASUSTeK/Broadcom 440x 10/100 Ir Configure
This cg	nnection uses the following items:
	Client for Microsoft Networks File and Printer Sharing for Microsoft Networks QoS Packet Scheduler Internet Protocol (TCP/IP)
	nstall Uronetall Properties
Tran wide	ription ismission Control Protocol/Internet Protocol. The default area network protocol that provides communication ss diverse interconnected networks.

4. Select **Obtain an IP address automatically** and **Obtain DNS server address automatically**.

Internet	Protocol (TCP/IP) Prope	rties	? 🔀
General	Alternate Configuration		
this cap	n get IP settings assigned auton pability. Otherwise, you need to a propriate IP settings.		
<u>o</u>	btain an IP address automaticall	y	
OU	se the following IP address:		
JP ad	ddress:		
Sub	netmask		
<u>D</u> ela	aul) galeway.		
00	<u>b</u> tain DNS server address autor	natically	
OU:	s <u>e</u> the following DNS server add	Iresses:	
Erete	ened DNS server		
Alten	mate DNS server		
		Advan	ced
		ОК	Cancel

For MacOs

- 1. Double click on the current used MacOs on the desktop.
- 2. Open the **Application** folder and get into **Network**.
- 3. On the **Network** screen, select **Using DHCP** from the drop down list of Configure IPv4.

		Net	work		
show All	Displays Sou	d Network	isk		
	Lo	cation: Automatic		;	
		Show: Built-in Eth		•	
Co	nfigure IPv4:	P PPPoE Apple Using DHCP	Talk Proxies E	thernet	
	IP Address:	192.168.1.10	(Renew DHC	P Lease
5	Subnet Mask: Router:	255.255.255.0	DHCP Client ID:	(If required)	
	DNS Servers:	192.108.1.1			(Optional)
Sear	ch Domains:				(Optional)
I	Pv6 Address:	fe80:0000:0000:000	0:020a:95ff:fe8d:7	2e4	
		Configure IPv6			(?)

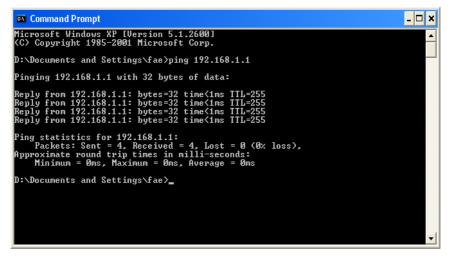
6.3 Pinging the Router from Your Computer

The default gateway IP address of the router is 192.168.1.1. For some reason, you might need to use "ping" command to check the link status of the router. **The most important thing is that the computer will receive a reply from 192.168.1.1.** If not, please check the IP address of your computer. We suggest you setting the network connection as **get IP automatically**. (Please refer to the section 4.2)

Please follow the steps below to ping the router correctly.

For Windows

- 1. Open the **Command** Prompt window (from **Start menu> Run**).
- 2. Type **command** (for Windows 95/98/ME) or **cmd** (for Windows NT/ 2000/XP). The DOS command dialog will appear.



- 3. Type ping 192.168.1.1 and press [Enter]. If the link is OK, the line of **"Reply from 192.168.1.1:bytes=32 time<1ms TTL=255"** will appear.
- 4. If the line does not appear, please check the IP address setting of your computer.

For MacOs (Terminal)

- 1. Double click on the current used MacOs on the desktop.
- 2. Open the Application folder and get into Utilities.
- 3. Double click **Terminal**. The Terminal window will appear.
- 4. Type **ping 192.168.1.1** and press [Enter]. If the link is OK, the line of **"64 bytes from 192.168.1.1: icmp_seq=0 ttl=255 time=xxxx ms**" will appear.

000	Terminal = bash - 80x24	
64 bytes from 192.168.3 64 bytes from 192.168.3 64 bytes from 192.168.3 64 bytes from 192.168.3	g 192.168.1.1 168.1.1): 56 data bytes 1.1: icmp_seq=0 ttl=255 time=0.755 ms 1.1: icmp_seq=1 ttl=255 time=0.697 ms 1.1: icmp_seq=2 ttl=255 time=0.716 ms 1.1: icmp_seq=3 ttl=255 time=0.731 ms 1.1: icmp_seq=4 ttl=255 time=0.72 ms	8
the second s	5 packets received, 0% packet loss = 0.697/0.723/0.755 ms	

6.4 Checking If the ISP Settings are OK or Not

Click Internet Access group and then check whether the ISP settings are set correctly.



For PPPoE Users

1. Check if the **Enable** option is selected.

Internet Access >> PPPoE

2. Check if **Username** and **Password** are entered with correct values that you **got from** your **ISP**.

PPPoE Setup		PPP/MP Setup
PPOE Link ISP Access Setup ISP Name Username Password WAN Connection D Mode Ping IP TTL: WAN Backup Setup 3G USB Modem	ARP Detect	PPP Authentication PAP or CHAP ♥ ♥ Always On Idle Timeout -1 second(s) IP Address Assignment Method (IPCP) WAN IP Alias Fixed IP ○ Yes ● No (Dynamic IP) Fixed IP Address ● Default MAC Address ● Specify a MAC Address MAC Address: 00 .50 .7F :9A .32 .71
Dial Backup Go to 3G US	Mode Disable 🚩	

For Static Users

1. Check if the **Enable** option for Broadband Access is selected.

Internet Access >> Static or Dynamic IP

Static or Dynamic IP (DHCP Client)	
Access Control	WAN IP Network Settings WAN IP Alias
Broadband Access	Obtain an IP address automatically
Keep WAN Connection Enable PING to keep alive PING to the IP 0.0.0.0 PING Interval 0 minute(s) WAN physical type Auto negotiation	Router Name * Domain Name * * : Required for some ISPs * Specify an IP address 192.168.5.29 Subnet Mask 255.255.255.0 Gateway IP Address 192.168.5.1
WAN Connection Detection Mode ARP Detect v Ping IP	 Default MAC Address Specify a MAC Address MAC Address: .50 .7F :9A .32 .71
RIP Protocol Enable RIP WAN Backup Setup 3G USB Modem Dial Backup Mode Go to <u>3G USB Modem</u> Setup	DNS Server IP Address Primary IP Address Secondary IP Address

- 2. Check if **WAN IP Network Settings** is set appropriately.
- 3. Check if **IP** Address, Subnet Mask and Gateway are set correctly (must identify with the values from your ISP) if you choose Specify an IP address.

For PPTP Users

1. Check if the **Enable** option for **PPTP** Link is selected.

Internet Access >> PPTP

PPTP Client Mode	
PPTP Setup	PPP Setup
PPTP Link 🔿 Enable 💿 Disable	PPP Authentication PAP or CHAP
PPTP Server 10.0.0.138	Always On
ISP Access Setup	Idle Timeout -1 second(s)
Username 123	IP Address Assignment Method (IPCP)
	Fixed IP O Yes No (Dynamic IP)
Password •••	Fixed IP Address
	WAN IP Network Settings
WAN Backup Setup	 Obtain an IP address automatically
3G USB Modem	Specify an IP address
Dial Backup Mode Disable Y	IP Address 192.168.5.29
Go to <u>3G USB Modem Backup</u> Setup	Subnet Mask 255.255.255.0
·	OK

- 2. Check if **PPTP Server, Username,** and **Password** are set correctly (must identify with the values from your ISP).
- 3. Check if **WAN IP Network Settings** are set properly. If you select **Specify an IP address**, you have to type in the values of **IP Address** and **Subnet Mask** manually. Be sure the values that you type identify with the values from your ISP.

6.5 Problems for 3G Network Connection

When you have trouble in using 3G network transmission, please check the following:

Check if USB LED lights on or off

You have to wait about 15 seconds after inserting 3G USB Modem into your Vigor2110. Later, the USB LED will light on which means the installation of USB Modem is successful. If the USB LED does not light on, please remove and reinsert the modem again. If it still fails, restart Vigor2110.

USB LED lights on but the network connection does not work

Check the PIN Code of SIM card is disabled or not. Please use the utility of 3G USB Modem to disable PIN code and try again. If it still fails, it might be the compliance problem of system. Please open DrayTek Syslog Tool to capture the connection information (WAN Log) and send the page (similar to the following graphic) to the service center of DrayTek.



AN Status TX Packets RX Packets 0 6442 3807 WAN IP (Static) RX Packets 6442 3807 0	kets TX Rate
6442 3807 0 eWall Log VPN Log User Access Log Call Log WAN Log Network Infomation Net State Time Host Message	
e Wall Log VPN Log User Access Log Call Log WAN Log Network Infomation Net State Time Host Message	0
Time Host Message	
Time Host Message	
	<u>^</u>
Apr 12 09:17:49 Vigor WAN2 PPPoE <= Protocol:LCP(c021) ConfReq Identifier:0x03	ACCM: 0x0 Authe:
Apr 12 09:17:49 Vigor [3G]Modem status:a1 20 00 00 00 02 00 03 00	MDH 1500 ACCh
Apr 12 09:17:49 Vigor WAN2 PPPoE => Protocol:LCP(c021) ConfReq Identifier:0x00 Apr 12 09:17:49 Vigor WAN2 PPPoE <= V:1 T:1 PADS ID:0	MRU: ISUU ACCM
Apr 12 09:17:49 Vigor WAN2 PPPoE <= V:1 T:1 PADS ID:0 Apr 12 09:17:49 Vigor [3G]Modem response: CONNECT 3600000	
Apr 12 09:17:49 Vigor [36]Modem response: CONNECT 5000000	
Apr 12 09:17:49 Vigor [3G]Modem status:a1 20 00 00 00 02 00 02 00	
Apr 12 09:17:49 Vigor [3G]Modem dial ATDT*99#	
Apr 12 09:17:49 Vigor WAN2 PPPoE => V:1 T:1 PADR ID:0	
Apr 12 09:17:49 Vigor WAN2 PPPoE <= V:1 T:1 PADO ID:0	
Apr 12 09:17:49 Vigor [3G]Modem response: OK	
Apr 12 09:17:49 Vigor [3G]Modem initialize A T&FE0V1X1&D2&C1S0=0	
Apr 12 09:17:49 Vigor WAN2 PPPoE => V:1 T:1 PADI ID:0	<u>~</u>
	>

Transmission Rate is not fast enough

Please connect your Notebook with 3G USB Modem to test the connection speed to verify if the problem is caused by Vigor2110. In addition, please refer to the manual of 3G USB Modem for LED Status to make sure if the modem connects to Internet via HSDPA mode. If you want to use the modem indoors, please put it on the place near the window to obtain better signal receiving.

6.6 Backing to Factory Default Setting If Necessary

Sometimes, a wrong connection can be improved by returning to the default settings. Try to reset the router by software or hardware. Such function is available in **Admin Mode** only.

8

Warning: After pressing **factory default setting**, you will loose all settings you did before. Make sure you have recorded all useful settings before you pressing. The password of factory default is null.

Software Reset

You can reset the router to factory default via Web page.

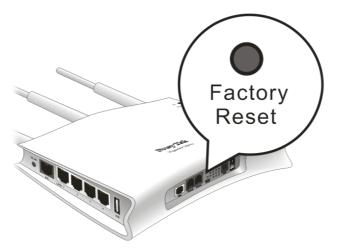
Go to **System Maintenance** and choose **Reboot System** on the web page. The following screen will appear. Choose **Using factory default configuration** and click **OK**. After few seconds, the router will return all the settings to the factory settings.

System Maintenance >> Reboot System

Do you want to reboot your router ?
Osing current configuration
O Using factory default configuration

Hardware Reset

While the router is running (ACT LED blinking), press the **Factory Reset** button and hold for more than 5 seconds. When you see the **ACT** LED blinks rapidly, please release the button. Then, the router will restart with the default configuration.



After restore the factory default setting, you can configure the settings for the router again to fit your personal request.

6.6 Contacting Your Dealer

If the router still cannot work correctly after trying many efforts, please contact your dealer for further help right away. For any questions, please feel free to send e-mail to support@draytek.com.

